The Reliance on Artificial Intelligence Measures to Curb Money Laundering Practices in the South African Banking Institutions and Real Estate Sector[1]

Howard Chitimira[2]

Abstract: Money laundering includes any practice by which illicit perpetrators disguise the original ownership and control of their proceeds of criminal conduct by making them appear to have been derived from legitimate sources. Money laundering practices may give rise to poor market integrity and low public investor confidence in any country. Consequently, money laundering is outlawed in many countries, including South Africa. On the other hand, artificial intelligence (AI) could be defined as the simulation of human intelligence processes by computer systems and/or machines in order to learn or acquire certain information, reasoning and related rules, and/or applying such rules to reach approximate or definite conclusions and self-correction. Put differently, AI also involves the creation of intelligent machines that perform and react like humans. Accordingly, the article unpacks the flaws in the current South African anti-money laundering statutory regulatory framework. This done to, *inter alia*, recommend the use of artificial intelligence and other relevant measures to enhance the combating of money laundering in the South African banking and related financial institutions. In light of this, the author submits that South African banks should consider adopting artificial intelligence measures to detect and prevent the negative effects of money laundering in the banking sector, and related key sectors such as the real estate and financial markets sectors.

Keywords: artificial intelligence; machine learning; money laundering; banks, automation

1. Introduction

Various definitions, enforcement approaches and interpretations of the concept of money laundering have to date been employed by anti-money laundering enforcement bodies in both developed and developing countries such as the United

[1] This article is based on the research supported in part by the National Research Foundation of South Africa (NRF) (Grant Number: 112115). Consequently, the author wishes to thank the NRF for its valuable support.

[2] Professor, Securities and Financial Markets Law, North West University, South Africa. Address: Potchefstroom Campus, 11 Hoffman Street, Potchefstroom 2531, South Africa, Corresponding author: howard.chitimira@nwu.ac.za.

States of America (USA), the United Kingdom (UK), Australia and South Africa. Nonetheless, for the purposes of this article, money laundering includes any practice by which illicit perpetrators disguise the original ownership and control of their proceeds of criminal conduct by making them appear to have been derived from legitimate sources (de Koker 2003). Money laundering practices may give rise to poor market integrity and low public investor confidence in any country. Consequently, money laundering is outlawed in many countries, including South Africa (p.s 3-4 & 20A-71 of the Financial Intelligence Centre Act 38 of 2001 as amended by the Financial Intelligence Centre Amendment Act 1 of 2017 (FICA); ss 2-24 of the Protection of Constitutional Democracy against Terrorist and Related Activities 33 of 2004 (POCDATARA) and ss 4-70 of the Prevention of Organised Crime Act 121 of 1998 as amended (POCA)). On the other hand, artificial intelligence (AI) could be defined as the simulation of human intelligence processes by computer systems and/or machines in order to learn or acquire certain information, reasoning and related rules, and/or applying such rules to reach approximate or definite conclusions and self-correction (Goldfarb & Prince, 2008). Put differently, AI also involves the creation of intelligent machines that perform and react like humans (p.mith *et al*, 2006). There are several types of AI and its examples includes automation, machine learning (deep learning, supervised and unsupervised learning, reinforcement learning), machine vision, natural language processing, robotics and self-driving cars. AI may also be utilised in searching knowledge, planning, problem solving and moving objects. Given this background, it is submitted that the FICA must be amended to introduce provisions that specifically obliges banking institutions to adopt and use AI measures to curb money laundering. These AI measures could also be employed to detect and prevent money laundering in the banks, real estate sector and the financial markets of South Africa (Goldfarb & Prince, 2008). This approach could further enable enforcement authorities to timeously and effectively detect any series of multiple transactions in the real estate sector, financial markets and/or banking institutions that are normally used to disguise the source of illicit financial assets and profits by the perpetrators of money laundering in South Africa (de Koker, 2009). The article explores the flaws in the current South African anti-money laundering statutory regulatory framework. Accordingly, the role and functions of the Financial Intelligence Centre (FIC) and other relevant enforcement bodies are discussed. This is done to, *inter alia*, recommend the use of artificial intelligence and other relevant measures to enhance the combating of money laundering in the South African real estate sector, financial markets and banking institutions. Moreover, the possible advantages and

disadvantages of the use of artificial intelligence measures to curb money laundering in such institutions, financial markets and the real estate sector are discussed.

2. Overall Aim

The article unpacks the flaws in the current South African anti-money laundering statutory regulatory framework. This done to, *inter alia*, recommend the adoption and use of AI measures to enhance the combating of money laundering activities in the South African real estate sector, financial markets and banking institutions.

3. Methodology

For the purposes of this article, a qualitative research methodology is employed. Accordingly, no quantitative and/or empirical research methods are used in the entire article. The article is mainly focused on the statutory analysis of the current South African anti-money laundering regulatory framework. Consequently, flaws in the current statutory regulatory framework are isolated in order to recommend the use of AI measures to detect and combat money laundering activities in the real estate sector, banks and/or financial markets in South Africa.

4. The Use of AI Measures and Money Laundering Regulation under the FICA

The FICA outlaws money laundering activities and the financing of terrorist practices in South Africa (p. 3(1) read with ss 2; 3(2); 4; 5; 20A-71 of the FICA). For instance, the FICA empowers the FIC to, *inter alia*, detect and take appropriate measures to identify proceeds of illicit activities in order to combat money laundering and the financing of terrorist activities in South Africa (p. 3(1) (a) & (b) of the FICA; de Koker 2011). The FIC is also authorised to impose appropriate financial sanctions against money laundering offenders pursuant to the adopted resolutions of the United Nations Security Council (Chapter VII of the United Nations Charter of 24 October 1945; also see s 3(1) (c) read with ss 26A-26C of the FICA). In addition, the FIC is obliged to investigate any suspected money laundering activities in South Africa and share any such information with other relevant persons such as investigating authorities, the National Director of Public Prosecution (NDPP) or the National Prosecuting Authority (NPA), intelligence service agencies,

the South African Revenue Service (p.ARS), the Independent Police Investigative Directorate, the Intelligence Division of the National Defence Force, the Special Investigating Unit, any investigative division in an organ of state and the Public Protector (p. 3(2) (a) read with s 4(b) of the FICA). The FIC is also required to share its information on suspected money laundering activities and financing of terrorist activities with similar bodies in other countries (p. 3(2) (b) of the FICA). This suggests that the anti-money laundering provisions of the FICA have extra-territorial application. The FIC may also take measures that require accountable institutions to freeze property and transactions of the offenders in accordance with the financial sanctions that may be imposed under the resolutions of the United Nations Security Council (p. 3(2) (aA) read with s 26A-26C of the FICA). Over and above, the FIC supervises other institutions and enforces compliance with the provisions of the FICA (p. 3(2) (c)). The FIC is further obliged to advise, inform and co-operate with other regulatory bodies and agencies on any matter regarding money laundering and terrorist financing activities in South Africa (p. 4(a); (aA) & (b) of the FICA). The FIC also monitors accountable institutions, supervisory bodies and other relevant persons to enhance their compliance with the anti-money laundering provisions of the FICA (p. 4(c) & (cA) read with subsections (d)-(g) & (5)). Notably, accountable institutions include practitioners, board of executors or a trust company, estate agents, authorised users of an exchange, managers of registered collective investment schemes, banks, mutual banks, money remitters, loan providers and foreign exchange dealers (p.chedule 1 read with ss 43B; 44 & 45 of the FICA).

The FICA prohibits banks and other accountable institutions from developing business relationships and/or concluding transactions with anonymous clients as well as clients acting under false and/or fictitious names (p. 20A). Accountable institutions are also obliged to establish and verify the identity of their clients prior to the establishment of any business relationship and/or conclusion of any transaction (p. 21 read with s 21A of the FICA). The accountable institutions must further establish the nature of their client's business and its ownership and control structure (p. 21 B (1) of the FICA). Where the client is a legal person, the accountable institution must establish the identity of the beneficial owner of the client by, *inter alia*, establishing the identity of each natural person who, independently or together with another person, has a controlling ownership interest in that legal person (p. 21B (2) (a) (i) of the FICA). Moreover, if the client is a legal person, the accountable institution must establish the identity of each natural person who exercises control of that legal person through other means; or determine the identity of each natural person who otherwise exercises control over the management of the legal person,

including in his or her capacity as the executive officer, non-executive director, independent non-executive director, director or manager (p. 21 B (2) (a) (ii) & (iii) of the FICA). Furthermore, where the client is a legal person, the accountable institution must take reasonable steps to verify and ascertain the identity of the beneficial owner of that client (p. 21 B (2) (b) of the FICA).

Where a natural person is acting on behalf of a partnership between natural persons, an accountable institution must establish the name of the partnership and verify the identity of all the partners and other relevant persons (p. 21 B (3) of the FICA). Likewise, where a natural person is acting in pursuance of the provisions of a trust agreement between natural persons, an accountable institution must establish and verify the name and number of the trust, the address of the Master of the High Court where the trust is registered, the identity of the founder, trustee, beneficiaries and other relevant persons of that trust (p. 21 B (4) of the FICA). Interestingly, the aforesaid due diligence provisions on legal persons, trusts and partnerships have extra-territorial application (p. 21 B (5) of the FICA). An accountable institution must conduct ongoing due diligence in respect of a business relationship which includes monitoring of transactions undertaken throughout the course of the relationship, checking the source of funds and keeping relevant information to ensure that the transactions are consistent with the accountable institution's knowledge of the client's business and risk profile (p. 21 C (a) & (b) read with s 21 D of the FICA). If an accountable institution is unable to establish and verify the identity of their client or obtain the information contemplated in section 21A or conduct ongoing due diligence as contemplated in section 21C, it must terminate existing business relationship and/or stop establishing new business relationships or concluding any transactions with that client (p. 21 E of the FICA). The accountable institution is further obliged to keep customer due diligence records (p. 22 of the FICA), records of each transaction (p. 22 A of the FICA), for at least five years from the date on which that transaction and/or business relationship was concluded in electronic form that is capable of being legibly reproduced later (p.s 23 & 24 of the FICA). Access to information and records by authorised representatives, electronic transfers of money to or from South Africa as well as cash transactions above prescribed limit must be approved by the FIC (p.s 27; 27 A; 28; 30 & 31 of the FICA). Property associated with terrorist and/or related activities, financial sanctions pursuant to resolutions of United Nations Security Council and suspicious and unusual transactions must be reported to the FIC timeously so as to prevent and combat possible money laundering practices (p.s 28 A & 29 of the FICA). Thereafter, the FIC may refer such transactions to an investigating authority or the NDPP for further

investigations and/or prosecution (p. 34 (1) (b) (ii) of the FICA). Notably, the FIC must make information reported to it, or obtained by it available to the NDPP, supervisory authorities and other regulatory bodies (p. 40 of the FICA). Be that as it may, the FIC is required to take appropriate measures to protect confidential and personal information of the suspected offenders in accordance with the FICA (p.s 41 & 41 A).

Accountable institutions must develop and implement adequate anti-money laundering and counter-terrorist financing risk management and compliance programmes that empowers such institutions to identify, assess, monitor and mitigate money laundering and terrorist activities risks optimally (p. 42 read with ss 42 A and 42 B of the FICA). Furthermore, accountable institutions are required to train their employees to enable them to consistently comply with the provisions of the FICA and the Risk Management and Compliance Programme (p. 43 of the FICA). The FIC or any relevant supervisory body may impose administrative sanctions on an accountable institution, reporting institution or other person that violates the relevant provisions of the FICA (p. 45 C (1) & (2)). Accordingly, the FIC or any relevant supervisory body may caution the offender not to repeat the conduct which led to the non-compliance, reprimand the offender, give a directive for remedial action or restriction or suspension of certain specified business activities or a financial penalty not exceeding R10 million in respect of natural persons or R50 million for juristic persons (p. 45 C (3) read with subsections (4)-(11) of the FICA).

Despite the regulatory efforts of the FICA as stipulated above, no provision of this Act specifically provides for the use of AI anti-money laundering measures in South Africa. This directly implies that the South African banking institutions are not statutorily obliged to adopt and/or employ AI measures to detect and combat money laundering practices. Consequently, this could also suggest that AI anti-money laundering measures are not expressly and statutorily utilised in banks, financial markets, real estate sector and other related sectors in South Africa. Put differently, machine learning and other AI measures are currently not used by banks and other related institutions to detect, monitor, assess and combat money laundering activities in the financial markets, real estate sector and related sectors in South Africa.

5. The Use of AI Measures and Money Laundering Regulation under the POCA

Money laundering, racketeering and other illicit activities are prohibited under the POCA (p.s 2-6). For instance, any person convicted of racketeering offences is liable to a fine not exceeding R100 million or to imprisonment for a certain period or to life imprisonment (p. 3 (1) of the POCA). Moreover, before the sentencing of the convicted racketeering offender, a regional court may impose a further penal fine not exceeding R100 million or imprisonment for a period not exceeding 30 years on that offender (p. 3 (2) (b) (i) of the POCA). The regional court may also refer the convicted offender for sentencing by the High Court where the purported penal fine exceeds a fine of R100 million or imprisonment for a period of 30 years or where it merits life imprisonment (p. 3 (2) (b) (ii) of the POCA). Furthermore, any person who engages in unlawful money laundering activities, transactions, agreements or receives property or any proceeds of unlawful activities and/or attempt to conceal or disguise the nature, source, location, disposition or movement of the said property or its ownership or any interest which anyone may have in respect thereof commits an offence (p. 4 of the POCA). Interestingly, any person that enables or assists another person who commits or has committed money laundering or other related offences in South Africa or elsewhere to avoid prosecution or remove or diminish any property acquired directly or indirectly from such offences will be liable for violating the provisions of the POCA (p. 4 (b) (ii)). This shows that the anti-money laundering provisions of the POCA have extra-territorial application.

Furthermore, any person who assist another person to receive benefits from the proceeds of unlawful activities such as money laundering will be guilty of an offence (p. 5 of the POCA). Any person who knowingly acquires, possess or uses property that is part of the proceeds of another person's unlawful money laundering activities will be liable for an offence (p. 6 of the POCA). However, persons accused of money laundering and related offences may escape liability if they successfully rely on the defence that they had reported their suspicions in terms of section 29 of the FICA (p. 7 A(1) of the POCA). The accused persons may also escape liability if they successfully raise the defence that they complied with the applicable obligations in terms of the internal rules of the accountable institution relating to the reporting of suspicious information. The accused persons may further escape liability if they prove that they reported the matter to their managers or persons charged with the responsibility of ensuring compliance with the provisions of the POCA by the accountable institution in question (p. 7 A (2) of the POCA). Notably, any person

convicted of money laundering and related offences will be liable to a fine not exceeding R100 million or to imprisonment for a period not exceeding 30 years (p. 8(1) of the POCA). Moreover, realisable property and affected gifts may be recovered from the offenders through civil court proceedings (p.s 13-17 read with ss 30-31 & 34-36 of the POCA). Accordingly, the courts may also impose confiscation orders and/or restraint orders against the offenders in respect of their illicit proceeds of money laundering and other related unlawful activities (p.s 18-29A of the POCA). This is usually done to recover and preserve the illicit proceeds and/or prohibit the offenders from destroying any property bought by such proceeds (p.s 38-45 of the POCA). Once the preservation of property order is obtained, the NDPP may apply to the High Court for an order forfeiting all proceeds of money laundering or any illicitly gained property to the state (p. 48(1) of the POCA).

Notwithstanding the anti-money laundering provisions of the POCA as highlighted above, the combating of money laundering has remained problematic in the financial services industry, especially in the banks and the real estate sector in South Africa to date (Kersop & du Toit, 2015). The recent mismanagement, governance, manipulation of financial statements and/or money laundering scandal that occurred at the Venda Building Society mutual bank (VBS bank) involving about R900 million that still cannot be accounted for and about R2 billion that was embezzled out of the bank by the offenders is a case in point. The Gupta family money laundering scandal between 2017 and 2018 involving several billions of South African rands that were siphoned out through the HSBC Holdings PLC, the Standard Chartered PLC and the Bank of Baroda South Africa is another example. The laundered money was reportedly used to buy companies, houses and other properties in Dubai and India. The failure by the banks to detect and prevent these money laundering activities could have been exacerbated by the fact that the POCA does not oblige banks to use AI anti-money laundering measures. In other words, the POCA does not have any provision that expressly empowers banks to employ machine learning, transaction monitoring systems and other AI measures to detect and combat money laundering activities that are perpetrated through banks, financial markets and the real estate sector (Carvalho, & Marzag˜ao, 2016).

6. The Use of AI Measures and Money Laundering Regulation under the POCDATARA

The POCDATARA does not expressly prohibit money laundering. Nonetheless, the POCDATARA outlaws terrorist activities and related offences associated with such activities (pp. 2-3). Thus, money laundering activities may only be outlawed under the POCDATARA if they are used to commit or help offenders to commit terrorism (Bester, Chamberlain, de Koker, Hougaard, Short, Smith & Walker 2008). The POCDATARA prohibits offences associated with the financing of terrorist activities (p. 4 read with pp. 2-3 of the POCDATARA). Thus, any person that engages in money laundering to support and finance terrorist activities will be liable for an offence under the POCDATARA (p. 4 read with pp. 2-3). Furthermore, any person who harbours or conceals another person whom he or she knows, or ought reasonably to have known or suspected to have committed terrorism or related offences will be guilty of an offence (p. 11 of the POCDATARA). The POCDATARA also places a duty on all persons to report the presence of any person suspected of committing or intending to commit terrorism and related offences to the relevant authorities in South Africa (p. 12(1)). Consequently, any failure to report terrorist suspects and/or those that are involved in the financing of terrorism activities will give rise to an offence under the POCDATARA (p. 12(2)). Likewise, any person who threatens or conspires with any other person, or aids, abets, induces, incites, instigates, instructs or commands, counsels or procures another person to commit terrorism or related offences will be liable for an offence under the POCDATARA (p. 14). The South African courts have jurisdiction over offences committed in South Africa. For the purposes of determining the jurisdiction of the court in respect of offences committed outside South Africa, the offence is deemed to have been committed at the place where the accused is ordinarily resident or where the accused has a principal place of business (p. 15(3) of the POCDATARA). Upon conviction, the offenders that finance terrorist activities may be liable for a High Court or a regional court fine not exceeding R100 million or to imprisonment for a period not exceeding 15 years or to a magistrate court fine not exceeding R250 000 or to imprisonment for a period not exceeding five years (p. 18(1) (c) of the POCDATARA). Moreover, any person convicted of terrorism is liable to a High Court fine or imprisonment for a period up to life imprisonment or to a regional court fine or imprisonment for a period not exceeding 18 years or to a magistrate court fine or imprisonment for a period not exceeding five years (p. 18(1) (a) of the POCDATARA). The courts may also impose freezing orders and/or order that the

property or proceeds of terrorist activities be forfeited to the state (p. 19, 22 & 23 of the POCDATARA).

The POCDATARA does not, however, expressly require banks to employ AI measures to detect, monitor, assess and combat money laundering activities in the financial markets, real estate sector and related sectors in South Africa. As a result, one can conclude that the ongoing money laundering challenges in South Africa could have been increased by the absence and/or non-use of AI anti-money laundering measures by the banks. Given this background, the sub-headings below explore possible advantages and disadvantages of using AI anti-money laundering measures in banks, financial markets and the real estate sector in South Africa.

7. Possible Advantages of AI Anti-Money Laundering Measures in Banks, Financial Markets and Real Estate Sector

Although AI has reportedly been existing as early as the 1950s, it has not yet gained much trust and usage in banks and related institutions to detect and prevent money laundering activities. South Africa's anti-money laundering laws only came into effect in 2002 (de Koker, 2008) and they were largely influenced by the Financial Action Task Force (FATF) recommendations. The FATF is an international anti-money laundering oversight body that provided its first set of recommendations for combating money laundering in 1990 (de Koker, 2008). The FATF also published its forty recommendations and related measures to curb money laundering and terrorist financing in 2001. The forty recommendations were later revised in 2003 to, *inter alia*, introduce risk-based principles and empower the relevant authorities to employ a risk-based approach to effectively curb money laundering and terrorism (de Koker, 2008). Nevertheless, both the FATF and the current South African anti-money laundering laws do not expressly provide for the use of AI measures in banks, financial markets and the real estate sector. In light of this, the possible advantages of AI anti-money laundering measures are discussed below.

AI anti-money laundering measures could provide timeous and effective detection and preventative solutions for banks and related institutions in South Africa. Thus, AI measures could transform and enhance the banks and related institutions' compliance with anti-money laundering laws in South Africa and elsewhere. The author concurs with the Financial Stability Board (FSB)'s submission that AI measures are largely developed through computer systems that are programmed and empowered to have some intelligence and to perform certain tasks. In light of this,

the author submits that AI anti-money laundering measures such as automation and machine learning should be employed in banks, financial markets and real estate sector to enhance the timeous detection and combating of money laundering activities in South Africa.

AI anti-money laundering measures could also equip banks and related financial institutions to effectively scrutinise and examine their customers' risk profile and detect suspicious transactions that may result in money laundering practices that are perpetrated through banks, real estate sector and financial markets. Put differently, AI anti-money laundering measures could enhance the Know Your Customer (KYC) rules and principles that require banks and related institutions to timeously detect, isolate and investigate high-risk customers so as to, *inter alia*, combat money laundering practices. If AI anti-money laundering measures are statutorily adopted in South Africa, banks and related institutions that do not comply with such measures and KYC rules should be fined and/or penalised.

AI anti-money laundering measures may increase consistency and streamline bureaucracy in banks and related institutions. These measures could enhance positive customer experiences while at the same time improving the detection of money laundering in the banks, financial markets and real estate sector.

Moreover, proper use of AI measures such as computational intelligence, artificial immune systems, machine learning, data mining, pattern recognition and fuzzy logic could enable banks to detect and combat organised and sophisticated money laundering practices associated with complex financial products, real estate sector and global financial markets (Dilek, Çakır & Aydın, 2015).

The AI anti-money laundering measures could also assist banks and related institutions to avoid manual, repetitive, data-intensive methods that are time consuming and less effective (Moodley, 2008). These measures could further ameliorate human effort that is usually employed in customer due diligence, screening and transaction monitoring of customers by banks when detecting and investigating money laundering activities in South Africa. The AI anti-money laundering measures may, if well utilised, enable banks to cut costs on investigation and other preventative measures. In other words, these measures will not only improve customer due diligence and risk assessment but will further enable banks to quickly adapt to the ever changing global financial factors and related risk factors affecting their customers. This is key to the effective combating money laundering and terrorist financing in South Africa.

8. Possible Disadvantages of AI Anti-Money Laundering Measures in Banks, Financial Markets and Real Estate Sector

Notwithstanding the advantages stated above, AI anti-money laundering measures could also have some shortcomings. For instance, it is generally believed that AI measures are expensive to install and/or utilise for some banks (Moodley, 2008). It is estimated that UK banks uses about GBP5 million every year in a bid to combat money laundering and related practices (UK National Crime Agency, 2018). This suggests that a lot of money may be needed to procure and effectively utilise AI anti-money laundering measures. Consequently, AI measures are not yet widely utilised by banks to detect and combat money laundering in South Africa and other countries (Abdelhamid, Khaoula & Atika, 2014).

AI anti-money laundering measures may be difficult and too sophisticated to enforce. For instance, such measures require sufficient persons with the relevant expertise and adequate financial resources for them to effectively curb money laundering in any country. AI anti-money laundering measures such as unsupervised machine learning algorithms, data mining, pattern recognition and fuzzy logic are still very new to the banking sector, real estate sector and financial markets. This gives room for possible errors in their utilisation, particularly in developing countries such as South Africa. In this regard, the author submits that banks and related institutions should carefully plan and train their employees on how to effectively rely on AI anti-money laundering measures without creating undue burdens and/or costly errors to the detriment of their clients (Kingdon, 2004).

It is further submitted that AI anti-money laundering decisions may be enforced in a way that could be difficult to comprehend for other persons that do not understand the operation of AI measures. This follows the fact that banks and related institutions are usually obliged to furnish interested persons and/or accused persons with sufficient information on how and why they suspect that they committed money laundering or supported such activities after the decision to investigate or impose appropriate fines is undertaken. Thus, AI anti-money laundering measures could breed new interpretation and credibility problems for banks and other related institutions. Once this occurs, a potential risk of creating new problems through the reliance on complex AI anti-money laundering measures is inevitable.

Moreover, AI anti-money laundering measures could also repeat the pre-existing human errors, biases and shortcomings pertaining to the detection and prevention of money laundering activities. For instance, AI money laundering measures may only

function in accordance with the systems that are programmed into such measures. Accordingly, such measures could further give rise to unforeseen compliance and reputational problems for banks and related institutions if they are not effectively utilised. The dilemma is that rigid pre-loaded systems usually restrict the intelligence of the AI measures and/or machines in question to the pre-loaded systems alone. On the other hand, overly flexible AI anti-money laundering measures could result in numerous legal challenges that ensue from those whose rights are violated by such measures when they malfunction (Álvarez-Jareño, Badal-Valero & Pavía-Miralles 2017). In light of this, banks and related institutions should strike a healthy between too rigid and/or too flexible AI anti-money laundering measures prior to their enforcement in South Africa.

AI anti-money laundering measures may create data protection problems in respect of sensitive personal data that is usually collected from customers by banks and/or related institutions during customer due diligence and/or related approaches that are employed to enforce anti-money laundering laws in South Africa (Mugarura 2014). In relation to this, the European Union (EU) General Data Protection Regulation (GDPR) [2016/679] OJL127, 23/5/2018, has commendably attempted to address some of the data-related challenges faced by EU member states, in respect of automated decision making. For instance, the GDPR allows full automated decisions against natural persons only in certain exceptional circumstances (article 22). Thus, South African banks and anti-money laundering regulatory bodies should carefully employ AI measures to avoid violating data and privacy rights of the accused persons (Woodsome & Ramachandran 2018).

Lastly, AI anti-money laundering measures may result in accountability and vicarious liability on the part of the banks and related institutions. For instance, if a bank employs AI anti-money laundering measures that wrongly suggest a certain individual has committed or supported money laundering, the bank should be held vicariously liable for its faulty AI measures (Ezrachi & Stucke 2017).

9. Concluding Remarks

South Africa has made commendable efforts to comply with the FATF recommendations on the combating of money laundering and terrorist financing by enacting anti-money laundering laws such as the FICA, the POCA and the POCDATARA. These statutes have been amended numerous times in a bid to keep up with the international standards and revamp the anti-money laundering statutory regulatory framework in South Africa. While these developments are welcome, more still needs to be done to improve the detection, investigation and curbing of money laundering activities in South Africa. For instance, despite the possible disadvantages of AI measures stated above, South Africa should seriously consider introducing such measures to effectively curb money laundering in banks, real estate sector and financial markets. In this regard, it is submitted that the FICA, the POCA and the POCDATARA should be amended to expressly enact provisions that obliges banks and related institutions to carefully use AI anti-money laundering measures in the real estate sector and financial markets. As earlier stated, this approach could enable banks and related institutions to timeously detects and prevent money laundering practices in South Africa. If well implemented, AI anti-money laundering measures could further empower South African banks and related financial institutions to effectively examine their customers' risk profile and combat money laundering practices that are perpetrated through banks, real estate sector and financial markets. In a nutshell, the author submits that AI anti-money laundering measures should be carefully and statutorily adopted in South Africa to maximise their advantages and avoid the possible disadvantages as discussed above.

References

Abdelhamid, D.; Khaoula, S. & Atika, O. (2014). Automatic Bank Fraud Detection Using Support Vector Machines. *International Conference on Computing Technology and Information Management Proceedings*. Dubai, pp. 10-17.

Álvarez-Jareño, J. A.; Badal-Valero, E. & Pavía-Miralles, J. M. (2017). Using Machine Learning for Financial Fraud Detection in The Accounts of Companies Investigated for Money Laundering. *Universitat Jaume Working Paper Series*, pp. 1-18.

Bester, H.; Chamberlain, D.; de Koker, L.; Hougaard, C.; Short, R.; Smith, A. & Walker, R. (2008). Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines. *Genesis Analytics*, 5(2), pp. 1-88.

de Koker, L. (2009). The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines. *Journal of Money Laundering Control*, 12(4), pp. 323-339.

de Koker, L. (2008). Money Laundering and Terror Financing Risk Management of Low Risk Financial Products and Services in South Africa. *Centre for Financial Regulation and Inclusion (Cenfri) Report for FinMark Trust*, pp. 3-32.

de Koker, L. (2003). Money Laundering Control: The South African Model. *Journal of Money Laundering Control*, 6(2), pp. 166-181.

de Koker, L. (2011). Will RICA's Customer Identification Data Meet Anti-money Laundering Requirements and Facilitate the Development of Transformational Mobile Banking in South Africa? An exploratory note. *Centre for Financial Regulation and Inclusion (CENFRI)*, South Africa, pp. 1-21.

Dilek, S.; Çakır, H. & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combat Cybercrimes: A Review. *International Journal of Artificial Intelligence & Applications*, 6(1), pp. 21-34.

Ezrachi, A. & Stucke, M. E. (2017). Artificial Intelligence and Collusion: When Computers Inhibit Competition. *University of Illinois Law Review*, 5, pp. 1775-1809.

Financial Action Task Force (2007). Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures. *High Level Principles and Procedures*, pp. 1-42.

Goldfarb, A. & Prince, J. (2008). Internet Adoption and Usage Patterns are Different: Implications for the Digital Divide. *Information Economics and Policy*, 20(1), pp. 2–15.

Kersop, M. & du Toit, S. F. (2015). Anti-money Laundering Regulations and the Effective Use of Mobile Money in South Africa – Part 1. *PER Journal*, 18(5), pp. 1603-1627.

Kingdon, J. (2004). AI Fights Money Laundering. *Applications: Banking*, pp. 87-89.

Moodley, M.S. (2008). Money Laundering and Countermeasures: A Comparative Security Analysis of Selected Case Studies with Specific Reference to South Africa. *Master of Security Studies, University of Pretoria*, pp. 1-93.

Mugarura, N. (2014). Customer Due Diligence (CDD) Mandate and the Propensity of its Application as a Global AML Paradigm. *Journal of Money Laundering Control*, 17(1), pp. 76-91.

Paula, E. L.; Ladeira, M.; Carvalho, R. N. & Marzag˜ao, T. (2016). Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering. *15th IEEE International Conference on Machine Learning and Applications*, pp. 954-960.

Smith C.; McGuire, B.; Huang, T. & Yang, G. (2006). The History of Artificial Intelligence. *University of Washington Research Paper*, pp. 1-27.

Woodsome, J. & Ramachandran, V. (2018). Fixing AML: Can New Technology Help Address the De-risking Dilemma? *Center for Global Development Paper Series*, pp. 1-83.

Legislation

Financial Intelligence Centre Act 38 of 2001 as amended.

Financial Intelligence Centre Amendment Act 1 of 2017.

Prevention of Organised Crime Act 121 of 1998 as amended.

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

National, Regional and Domestic Instruments and Reports

*** (2018). European Union General Data Protection Regulation (2016/679) OJL127, 23/5/2018.

*** (June 2007). Financial Action Task Force (Groupe d'action financière) *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing High Level Principles and Procedures*.

*** (1945). United Nations Charter of 24 October.