2023-04-27

Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era

Pavlidis, Georgios

Emerald Publishing Limited

Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era

Georgios Pavlidis
Faculty of Law, Neapolis University, Paphos, Cyprus

Received 7 March 2023
Revised 27 April 2023
Accepted 27 April 2023

Abstract

Purpose – This paper aims to critically examine the digital transformation of anti-money laundering (AML) and countering the financing of terrorism (CFT) in light of the Financial Action Task Force (FATF) San Jose principles, the Organisation for Economic Co-operation and Development (OECD) principles for artificial intelligence (AI) and the proposed European Union (EU) Artificial Intelligence Act. The authors argue that AI tools can revolutionize AML/CFT and asset recovery, but there is a need to strike a balance between optimizing AML efficiency and safeguarding fundamental rights.

Design/methodology/approach – This paper draws on reports, legislation, legal scholarships and other open-source data on the digital transformation of AML/CFT, particularly the deployment of AI in this context.

Findings – A new regulatory framework with robust safeguards is necessary to mitigate the risks associated with the use of new technologies in the AML context.

Originality/value – This study is one of the first to examine the use of AI in the AML/CFT context in light of the FATF San Jose principles, the OECD AI principles and the proposed EU AI Act.

Keywords Anti-money laundering (AML), Artificial intelligence (AI), Digitalization, Asset recovery, Know your customer (KYC), Transaction monitoring

Paper type Research paper

1. Introduction

The deployment of new technologies for anti-money laundering (AML) and countering the financing of terrorism (CFT) has been hailed as a "game changer" and an "up-and-coming revolution" (McKinsey and Company, 2022; KPMG, 2018). New technologies in this field are often referred to as regulatory technology (RegTech), for they promise to improve AML/CFT compliance and enhance the delivery of regulatory requirements through the use of artificial intelligence (AI) and its various subsets, such as machine learning and natural language processing (McCarthy, 2022; Brynjolfsson and McAfee, 2017; Stone *et al.*, 2016). Evidently, the ongoing digital transformation of AML/CFT must adhere to and keep pace with the relevant provisions of national and European Union (EU) laws, as well as the soft

This study was supported by the EU's Erasmus+ Programme. This publication reflects solely the author's views. The European Education and Culture Executive Agency (EACEA) and the European Commission are not responsible for any use of the information presented herein.

Journal of Money Laundering Control
Vol. 26 No. 7, 2023
pp. 155-166
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-03-2023-0050

law rules of the Financial Action Task Force (FATF), which is the key global standard-setter in the field of AML/CFT.

Such an adaptation is an arduous task for several reasons. AML/CFT compliance has been complicated due to the ever-increasing volume and complexity of cross-border transactions and the sophistication of money laundering techniques, as evidenced in numerous FATF reports over the past three decades (Pavlidis, 2021; FATF, 2015; FATF, 2010; FATF, 2008). The intricacy of AML/CFT compliance is also evidenced by the unremitting increase in the volume of suspicious activity reports (SARs) that authorities receive from regulated entities, especially financial institutions. In the USA alone, the SARs filed to the Financial Crimes Enforcement Network (FinCEN, 2000) increased from 100,000 in 2000 to 3.6 million in 2022, and there are no signs of a slowdown (U.S. Department of the Treasury, 2023; FinCEN, 2000). FinCEN and its counterpart Financial Intelligence Units (FIUs) around the globe must process millions of SARs efficiently and identify those that need to be forwarded to law enforcement agencies for further investigation, criminal proceedings and, ultimately, asset recovery. In addition to the increased number of SARs, AML/CFT compliance and the work of FIUs have been complicated by the evolving regulatory environment, the diversification of the normative sources of AML/CFT standards at the national and international levels and the proliferation of targeted sanctions against individuals and entities [1]. An additional burden on regulated entities and FIUs has been the gradual expansion of the scope of financial crimes in many jurisdictions, which may now cover tax evasion (e.g. UK Criminal Finances Act 2017) and bribery, sometimes with extraterritorial reach (e.g. UK Bribery Act 2010) (Saravalle, 2022; Chiu, 2017).

Faced with this heavy compliance burden, as well as increasingly aggressive AML enforcement in several jurisdictions, financial institutions must allocate more resources to support their compliance teams. To avoid hefty fines for non-compliance, they must be able to review a vast number of alerts generated by AML/CFT monitoring systems effectively and promptly (Amicelle, 2022; Partington, 2017). Consequently, financial institutions may need to spend up to 4% of their revenue on regulatory compliance (Walshe and Cropper, 2018; Duff and Phelps, 2017). Unsurprisingly, these alarming costs and risks have pushed the industry to explore new technological solutions for the digital transformation of AML/CFT compliance (LexisNexis Risk Solutions, 2016). As a result, investment in RegTech by leading financial institutions, Big Tech and start-ups is expected to reach US$115bn in 2023 and exceed 204bn by 2026, increasing considerably faster than the total amount spent for compliance as a whole (Juniper Research, 2022; Juniper Research, 2018; CBInsights, 2017).

Nevertheless, investment alone cannot ensure successful AML/CFT compliance. Standardization, clarity and consistency are also required. Indeed, to select the technological products that can best mitigate compliance risks, financial institutions need to rely on commonly accepted standards and principles for the digital transformation of AML/CFT, which are still lacking. This is particularly true when these institutions operate in multiple jurisdictions. Moreover, the emergence of new and specialized legislative frameworks, such as the proposed EU AI Act [2], might create a fragmented regulatory landscape in which the private sector and supervisors would need to navigate through various sets of rules and safeguards. This is particularly true when cross-border transactions and multiple jurisdictions are involved and/or when national regulations have an extraterritorial impact, as in the case of the aforementioned EU AI Act that has an impact outside the EU too. Thus, considerable standard setting work must be conducted for the digital transformation of AML/CFT, especially at the international level. This paper aims to contribute to this discussion by critically examining how new technologies can help the private sector and FIUs implement AML/CFT measures (Section 2) and what key principles should guide

responsible digital innovation in AML/CFT, considering the FATF San Jose principles, the Organisation for Economic Co-operation and Development (OECD) AI principles and the proposed EU AI Act (Section 3).

2. Digital transformation of AML/CFT for regulated entities and FIUs

The digital transformation of AML/CFT promises to help regulated entities, especially financial institutions, improve compliance with relevant national and international standards. For the sake of conciseness, we leave aside interesting digital innovations, such as electronic identity authentication (FATF, 2020; ITU, 2017), and focus on the use of AI-based tools in the AML/CFT context. We follow the OECD's definition of AI, which states that "an AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments ... with varying levels of autonomy" (OECD, 2019). Almost identically, the EU defines an AI system as "software that [...] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" [3]. Systems that fall within this category have the potential to improve AML/CFT compliance, particularly customer identification and transaction monitoring, although serious challenges remain for regulated entities and FIUs.

First, customer identification and identity management and control are key requirements of AML/CFT regulations (Arner *et al.*, 2019). Know-your-customer (KYC) requirements are set in national legislation [4] in line with international standards, particularly FATF Recommendation No. 10 and relevant binding instruments of international [5] and EU laws [6]. According to these standards, financial institutions and other regulated entities are required to undertake customer due diligence when establishing business relations (onboarding) and conducting transactions above a designated threshold. Regardless of thresholds, customer due diligence must be exercised when there is a suspicion of money laundering or terrorist financing or doubt about the veracity of customer or beneficial owner data. Enhanced due diligence and checks are also required for politically exposed persons (PEPs) and persons and entities targeted by sanctions (Scott, 2020; FATF, 2013). In the KYC context, AI-based tools can help financial institutions effectively detect fraud at the onboarding stage by improving client screening and risk rating. This is particularly important in view of the increase in identity fraud cases, with 15 million victims and US $24bn in illicit financial gains in 2022 in the USA alone (Javelin Strategy and Research, 2022). More specifically, AI-based tools can use data from various sources and in different languages (numerical data, documents, oral communications, biometric facial recognition, company and beneficial ownership registers, sanction watch lists, PEP registers, etc.) to improve KYC for persons engaging in identity fraud, persons and entities targeted by sanctions, PEPs and their entourages, etc. (FATF, 2021a; Breslow *et al.*, 2017). AI-based tools can also detect customers' native languages based on an analysis of written communications, identify tampered digital images or video sources (e.g. facial morphing) and capture customers' mobile phone GPS data to assess geographical money laundering risks (ESA, 2018).

Secondly, the use of AI is highly promising for transaction monitoring. National legislation and international standards, such as FATF Recommendation No. 20, impose on financial institutions and other regulated entities the obligation to detect, identify and report suspicious transactions to national FIUs, such as FinCEN in the USA. Failure to comply and file SARs may result in criminal and/or administrative sanctions. AI tools based on machine learning can enable regulated entities to promptly process large amounts of transaction data

in real time, analyse patterns of customer behaviour and identify anomalies and suspicious activity more quickly and accurately in accordance with each jurisdiction's reporting requirements. Adaptive behavioural analytics can build customers' baseline behavioural profiles by monitoring their transactions over time so that suspicious activities can be identified almost instantly (FATF, 2021a; Excell, 2019). Furthermore, statistical processes and predictive modelling (Hayble-Gomes, 2022) can be used to predict the likelihood of a transaction being fraudulent or part of a money laundering scheme without resorting to subjective human analysis. Thus, AI-based tools can increase the automation of monitoring and reporting processes and limit false alerts and the ensuing alert fatigue. Given that unreviewed alerts often accumulate due to the lack of experienced staff, it is estimated that AI-based tools can reduce false positives, currently representing 90% of alerts, to less than 50%, thereby reducing the workload of compliance teams and increasing the overall efficiency of AML defences (IIF, 2018; Breslow *et al.*, 2017).

According to the FATF, the problem is that financial institutions continue basing their risk assessments on "automated but static analyses of a pre-determined set of risk factors, together with human judgement". Moreover, the existing methods for generating matrixes for risk interpretation and action "very rarely offer a real-time overview of customer transactional or institutional risks". Furthermore, data cannot be analysed on a large scale and do not always offer "the accuracy and detail required to comply with AML/CFT standards" (FATF, 2021a). AI-based tools can offer a more dynamic analysis by combining customer information and real-time transaction data with data from multiple heterogeneous data sets, including invoices, bills of lading, email, regulatory data and other external data. To achieve this, shared tools need to be used, in compliance with data privacy legislation, to pool data from various firms to better trace transactions and the movement of funds across the financial industry (FATF, 2021b; FIRA, 2018). The challenge will be to identify weak signal patterns in vast volumes of data from various firms, with hundreds of transactions coming in each second. Among other promising fields, AI-based tools can uncover trade-based money laundering schemes by detecting unit prices in a series of transactions that diverge from established international thresholds in an attempt to overstate or understate the quantity of traded goods relative to payments (Herbert, 2022; FATF, 2006). In all cases, the key is to ensure adequate data pooling and sharing, collaborative analytics, as well as appropriate access by supervisors (FATF, 2021b).

Besides regulated entities, FIUs can also benefit from AI-based tools. The advantages of this digital transformation for FIUs are efficiency, quality, optimal resource deployment and a more dynamic risk-based approach (FATF and Egmont Group, 2021). In terms of efficiency, as FIUs receive and process large volumes of data from numerous reporting entities, AI-based tools can help them pool, sort and analyse more data quickly and efficiently. Regarding quality, FIUs must identify SARs of higher investigative value and prioritize them for analysis (Lagerwaard, 2023). According to the FATF, FIUs can resort to AI-based tools, such as supervised machine learning, which learn from the reports received, detect patterns, draw inferences and ultimately increase the quality of AML/CFT analysis (FATF and Egmont Group, 2021). Regarding resource deployment, FIUs' human resources are finite and need to be allocated in an optimal manner; therefore, there is an urgent need for digital tools that streamline data sorting and verification and other mundane tasks so that FIU analysts can focus on analytical tasks. With regard to the last advantage, AI-based tools can promote a more dynamic risk-based approach by supporting traditional risk analysis and identifying emerging risks that do not fall within already known profiles and typologies.

3. Mitigating risks: principles for the responsible use of AI in AML/CFT

If AI-based tools are not properly designed and deployed in the context of public authority, there is a risk of undermining "due process, equal protection and transparency" (Liu *et al.*, 2019). For instance, AI-based tools pose the risk of "flawed automated decision-making or profiling" (Data Protection Working Party, 2018) by regulated entities and FIUs due to subjective data inputs or selection bias (Feuerriegel *et al.*, 2020; Executive Office of the President, 2016). In this context, AI may amplify existing biases and discrimination. For example, in the fight against terrorism financing in the wake of the 9/11 terrorist attacks, financial institutions in the USA and other jurisdictions have used racial profiling and monitored activities as suspicious based on clients' (perceived) ethnicity (Lee, 2006). Besides the risk of bias, the deployment of AI in the AML/CFT context raises legitimate concerns about cyber resilience, data security, quality, consistency, completeness and privacy and the protection of fundamental rights. The sets of principles and rules discussed in the following subsections aim to mitigate risks and guide responsible digital innovation in AML/CFT.

3.1 The FATF San Jose principles

The San Jose guiding principles [7], the first set of non-binding principles (soft law) in this field, were formulated by the in FATF (2017) in the context of the ongoing dialogue between the FATF and the private sector, particularly the FinTech industry. The San Jose guiding principles reiterate the need to protect the financial system against the threats of money laundering and terrorism financing (Guiding Principle 1) through a collaborative framework and close engagement between governments and the private sector (Guiding Principle 2). They also encourage "positive and responsible innovation" (Guiding Principle 3) to increase the effectiveness of AML/CFT within a "smart" regulatory framework (Guiding Principle 4) that addresses risks without stifling innovation (Pavlidis, 2022). Nevertheless, these guidelines are rather vague and provide little clarity as to the specific characteristics of "responsible innovation" and "smart regulation". They also lack any reference to the protection of fundamental rights, which is perhaps the most serious shortcoming. Guiding Principle 5 briefly refers to the principles of fairness, commercial neutrality and consistency with the international regulatory environment; however, these are self-evident values that apply to all regulatory frameworks, not only to the use of AI in the AML/CFT context. On the positive side, the San Jose guiding principles constitute the first step in an ongoing process of consultations and must be viewed as a blueprint that can help establish more specific principles for the digital transformation of AML/CFT. Indeed, recent FATF reports (FATF, 2021c) go into more detail and stress the need for a risk-based approach to achieve a high degree of explainability and auditability and the protection of privacy and other human rights.

3.2 The OECD principles for AI and their application to AML/CFT

In 2019, the OECD developed its own set of guiding principles for the promotion of AI as an innovative and trustworthy technology that respects human rights and democratic values. The OECD principles treat AI as a general purpose technology – that is, not in the specific AML/CFT context (OECD, 2019). First, they state that AI should promote inclusive growth, sustainable development and well-being (OECD Principle 1), which is a general and uncontentious objective but offers little specific guidance. Secondly, they state that AI systems should be compatible with "the rule of law, human rights, democratic values and diversity" (OECD Principle 2), with a useful reference to the need for "appropriate safeguards, for example, enabling human intervention where necessary". The key challenge in this context is the establishment of effective mechanisms for informed oversight.

Informed regulation and supervision require developing expertise in new technologies, understanding the risks and being able to implement appropriate risk mitigation measures. Therefore, AML/CFT supervisors should be able to acquire such expertise to effectively supervise regulated entities' implementation of safeguards in their AI-based systems. The OECD principles also urge for more "transparency and responsible disclosure around AI systems" to allow people to challenge outcomes (OECD Principle 3), which is important as decisions made by AI tools are not always intelligible to humans who may be affected. In accordance with the "no tipping off" rule in the context of AML/CFT monitoring, individuals and entities are not informed about the AML/CFT alerts that target them [8]. In this context, transparency does not mean informing individuals flagged for suspicious transactions but requires that the methodology and outcomes of an AI model can be properly explained and communicated to the relevant AML authorities and supervisors. This is also related to the notions of auditability and explainability, which require that the results be reproducible when using the same inputs. Moreover, the OECD principles deal with security issues and the need to continuously assess and manage potential risks. This means that "in conditions of normal use, foreseeable use or misuse or other adverse conditions, [AI-based tools] function appropriately and do not pose unreasonable safety risks" (OECD Principle 4). This principle is very similar to the more detailed EU risk-based approach enounced in the proposed AI Act (see Section 3.3). Finally, the OECD principles state that individuals who develop, deploy or operate AI systems should be held accountable for their proper functioning (OECD Principle 5). In the AML/CFT context, this means that regulated entities and their compliance teams are responsible for compliance and for the functioning of their AI-based tools. This brings us to another important issue. AI-based tools should supplement – not replace – traditional AML/CFT mechanisms, such as transaction reporting (ESA, 2018), to allow compliance teams to focus on the analysis rather than on the collection and organization of large volumes of information from various sources. Financial institutions should not aim to eliminate the human element of AML/CFT; rather, they should seek to free up resources for higher-risk cases, supporting their analysts with AI-based tools without abdicating their responsibility (IIF, 2018) [9].

3.3 The proposed EU AI act and its application to AML/CFT

In April 2022, the European Commission presented its proposal for an EU AI Act that will be a binding legal instrument at the EU level, unlike the aforementioned soft law initiatives of the FATF and OECD. The EU initiative is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), the legal basis for EU instruments that ensure the establishment and functioning of the internal market. Indeed, AI constitutes a core part of the EU's digital single market, and there is a need for new harmonized rules on the development and use of AI-based products and services on this market. This also explains the choice of a regulation as a legal instrument, which ensures that the new rules on AI (definition, classification, prohibitions, etc.) will be applied directly and uniformly in accordance with Article 288 of the TFEU. The initiative aims to reduce the risk of legal fragmentation but also leaves some room for member states to choose how to organize their market surveillance systems and implement measures for promoting innovation in AI.

The proposed act is the first comprehensive legislative initiative for AI by a major regulator to ensure the transparency and explainability of processes and outcomes, as well as human oversight, cybersecurity, data protection and respect for privacy. Since December 2022 the text is waiting for the Council of the European Union and the European Parliament to finalize their positions before inter-institutional negotiations, which also include

representatives of the European Commission (trilogue). The Council's position (11 November 2022) contained useful adjustments proposed by the Czech presidency. Among these adjustments, the text's preamble states that the AI Act does not affect the powers and independence of national authorities and supervisors in the area of data protection or the protection of fundamental rights. Moreover, the adjustments emphasized the need for guidance by the European Commission on the application of the act's provisions, particularly the consistency of their enforcement across the EU, which will be, in our view, the key issue in the implementation phase, as is the case with most EU initiatives.

The core provisions of the proposed EU AI Act define a risk-based approach to AI, in which AI-related risks are classified as follows:

- unacceptable risk, such as social scoring, which will be prohibited under the AI Act;
- high risk, such as the use of AI in employee recruitment, medical devices, etc., which will be permitted subject to ex ante third-party assessment of conformity with AI requirements, taking into consideration relevant sectorial legislation;
- low-risk AI systems with specific transparency obligations, such as human impersonation by chatbots, which will be permitted subject to the obligation to notify humans that they are interacting with an AI system; and
- minimal- or no-risk AI applications, which will be permitted with no restrictions.

This risk-based approach involves carefully considering the potential risks and negative impacts of AI and taking steps to prevent or mitigate them. It can be argued that a risk-based approach to AI could be too limiting, thus undermining innovation (Renda, 2022). Nevertheless, we argue that this is not the case with the EU AI Act, which respects the principle of proportionality, for it imposes obligations and regulatory burdens only in cases in which AI systems pose high risks.

In the AML/CFT context, the provisions of the proposed EU AI Act will also apply to the use of AI by regulated entities and FIUs. The act and its risk classification are compatible with the FATF San Jose and OECD principles, which advocate for positive and responsible AI innovation, fairness, transparency and accountability. This is not surprising, given that most of the EU member states are also FATF and OECD members and help shape the work and initiatives of these bodies. The EU AI Act goes one step further by setting specific obligations, prohibitions and exceptions that apply horizontally to all AI systems across all sectors, thus including AML/CFT.

Regarding risk classification, the use of AI by regulated entities and FIUs in the AML/CFT context can be considered high-risk, as defined in Annex III sub-sections 6(e), (f) and (g) of the EU AI Act. Indeed, AI-based tools in the AML/CFT context target persons for the purpose of fighting crime and allow regulated entities and, ultimately, FIUs to search "complex related and unrelated large data sets available in different data sources or different data formats to identify unknown patterns or discover hidden relationships in the data" [10]. The use of AI for AML/CFT can be considered part of "crime analytics" because AML/CFT systems create alerts for certain clients and activities, which may later be forwarded to FIUs and thence to law enforcement authorities for further investigation, criminal proceedings and, ultimately, asset recovery. Therefore, the key provisions of the EU AI Act on high-risk AI also apply to AI systems in the AML/CFT context. As the AML/CFT sector is already regulated, the requirements stipulated by the AI Act will be integrated into existing processes and assessments by sectoral regulators. For instance, regulators will need to ensure that high-risk AI systems are effectively overseen by natural persons (Article 14 of the EU AI Act), which means that they should allow full manual analysis by the user at any

time ("stop" button) and make the reasoning behind the predictions and decisions made by AI accessible to human oversight (model explainability). This will ensure that the technology is used ethically and transparently – for example, by allowing the identification and correction of errors or biases in AML/CFT models – thus building trust in the use of AI. Regulated entities and FIUs that use AI-based tools will also need to ensure compliance with other key requirements of the AI Act, particularly high levels of data security and quality and the maintenance of adequate documentation to allow authorities to assess compliance. Consequently, regulated entities and FIUs will need to develop new operational governance structures and establish new roles, such as the role of AI compliance officer. For this reason, the transitional period following the entry into force of the EU AI Act must be proportionate to the new compliance burden imposed on the developers and users of AI-based tools.

4. Concluding remarks

One hundred years ago, Nobel Peace Prize laureate Christian Lange discerningly noted that "technology is a useful servant but a dangerous master" (Lange, 1921), warning that technological advancements may tempt states to wield unrestricted power. In the era of AI, this is a justifiable concern not only for states but also for the world's largest corporations, including Big Tech companies and major financial institutions. The financial and IT industries have already started revolutionizing AML/CFT compliance through AI to reduce regulatory risks and compliance costs and increase procedure efficiency. Indeed, the use of AI in AML/CFT can help detect and prevent money laundering by analysing vast amounts of financial data and identifying suspicious activity promptly and accurately. At the same time, however, it poses new regulatory challenges, including privacy, fairness, explainability and oversight (Bertrand *et al.*, 2021; FATF, 2021a). AML/CFT compliance must not degenerate into dystopian AI-assisted massive surveillance, allowing financial institutions to do what states cannot do directly.

For these reasons, it is essential to establish principles and rules for AI in AML/CFT to ensure that it is used responsibly and ethically. More specifically, it must be ensured that:

- transparency and accountability are guaranteed so that those who develop and use AI-based tools can be held responsible for any negative impacts;
- users and supervisors can understand how AI systems work and make decisions;
- AI systems are not used to perpetuate discrimination or bias; and
- privacy and data protection are taken into account in line with privacy laws and regulations.

The FATF San Jose and OECD principles move in this direction, but the EU AI Act takes more concrete regulatory action and sets specific horizontal rules on AI that also apply to AML/CFT.

A final factor to consider is the need for coordinated action at the national and international levels. Cooperation between competent authorities at the national level (FIUs, data protection and privacy authorities) is necessary to fully understand and mitigate the risks posed by the use of AI for AML/CFT; such cooperation may be both intragovernmental and public–private. International cooperation is necessary to promote the harmonization of rules, avoid legal fragmentation and ensure that the new technologies for AML/CFT remain aligned with global sectoral standards (AML/CFT, human rights, cybersecurity, data privacy, etc.). To this end, the deployment of AI in AML/CFT requires a continuous and constructive dialogue between policymakers, the financial industry and tech companies at the national and international levels. This is

unescapable because the role of AI in criminal acts, from cyberattacks to financial crimes, is very likely to increase (FATF, 2021a; Yeoh, 2019), and it will soon become imperative for regulated entities and FIUs to resort to more powerful AI tools and robust information sharing to counter the new threats. All things considered, a financial firm's or FIU's decision to invest in AI-based tools can pay dividends in the long term if these tools are used with the necessary robustness and consistency and in compliance with the emerging rules and principles for AI governance.

Notes

1. In the USA, the Office of Foreign Assets Control of the US Department of the Treasury administers an increasing number of sanctions programmes targeting foreign countries, regimes, companies and individuals suspected of terrorism, drug trafficking, money laundering, etc. See www.treasury.gov/resource-center/sanctions/Pages/legal-index.aspx (accessed 1 March 2023).
2. Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206 final
3. Article 3 par. 1 of the EU Artificial Intelligence Act.
4. See e.g. the UK Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (SI 2017 No. 692); French Ordinance no 2016-1635 (JORF No. 0280 of 2 December 2016), etc.
5. See e.g. Article 13 par. 2 of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention) of 2005.
6. See Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 156, 19.6.2018, p. 43.
7. San Jose Guiding Principles (2017), available at: www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-fintech-regtech-forum-may-2017.html; on the FATF FinTech and RegTech Initiative and the outcomes of the events organized by FATF, see: www.fatf-gafi.org/fr/publications/initiativefintechregtech/documents/?hf=10&b=0&s=desc(fatf_releasedate) (accessed 1 March 2023).
8. FATF Recommendation No. 21; Article 39 Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (consolidated text), OJ L 141, 5.6.2015, p. 73.
9. For a more technology-friendly approach, see Bunq v. De Nederlandsche Bank (DNB); in this 2022 case, the Dutch company appeal court (College van Beroep voor het bedrijfsleven) found that the online bank Bunq was complying with AML legislation by using AI-based tools for client screening.
10. According to these sections: "(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups; (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences; (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or different data formats to identify unknown patterns or discover hidden relationships in the data".

References

Amicelle, A. (2022), "Big data surveillance across fields: algorithmic governance for policing and regulation", *Big Data and Society*, Vol. 2022 No. 2, pp. 1-12.

Arner, D., *et al* (2019), "The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities", *European Business Organization Law Review*, Vol. 20 No. 1, pp. 55-80.

Bertrand, A., Maxwell, W. and Vamparys, X. (2021), "Do AI-based anti-money laundering (AML) systems violate European fundamental rights?", *International Data Privacy Law*, Vol. 11 No. 3, p. 276.

Breslow, S., *et al* (2017), *The New Frontier in anti–Money Laundering*, McKinsey and Company Brief.

Brynjolfsson, E. and McAfee, A. (2017), "What's driving the machine learning explosion", Harvard Business Review, available at: https://hbr.org/2017/07/whats-driving-the-machine-learning-explosion (accessed 1 March 2023).

CBInsights (2017), *Regtech Startups on Pace for Record Deals, against Backdrop of Shifting Regulatory Landscape*, Research Brief.

Chiu, I. (2017), "A new era in FinTech payment innovations? A perspective from the institutions and regulation of payment systems", *Law, Innovation and Technology*, Vol. 9 No. 2, pp. 190-234.

Data Protection Working Party (2018), "Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679", *Guidelines*, Vol. 17, p. 251.

Duff and Phelps (2017), *Global Regulatory Outlook Viewpoint*, Research Brief.

European Supervisory Authorities (2018), "Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process", ESA Opinion JC 2017 81.

Excell, D. (2019), "Using adaptive behavioral analytics to detect fraud", Risk Management Monitor, available at: www.riskmanagementmonitor.com/using-adaptive-behavioral-analytics-to-detect-fraud (accessed 1 March 2023).

Executive Office of the President (2016), "Big data: a report on algorithmic systems, opportunity, and civil rights", *Executive Office of the President Report*.

FATF and Egmont Group (2021), *Digital Transformation of AML/CFT for Operational Agencies*, FATF Report, Paris.

FATF (2006), *Trade-Based Money Laundering*, FATF Report, Paris.

FATF (2008), *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, FATF Report, Paris.

FATF (2010), *Money Laundering Using New Payment Methods*, FATF Report, Paris.

FATF (2013), *Politically Exposed Persons*, FATF Guidance, Paris.

FATF (2015), *Emerging Terrorist Financing Risks*, FATF Report, Paris.

FATF (2017), *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, FATF Report, Paris.

FATF (2020), *Guidance on Digital Identity*, FATF Guidance, Paris.

FATF (2021a), *Opportunities and Challenges of New Technologies for AML/CFT*, FATF Report, Paris.

FATF (2021b), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*, FATF Report, Paris.

FATF (2021c), *Suggested Action to Support New Technology for AML/CFT*, FATF Report, Paris.

Feuerriegel, S., Dolata, M. and Schwabe, G. (2020), "Fair AI: challenges and opportunities", *Business and Information Systems Engineering*, Vol. 62 No. 4, pp. 379-384.

Financial Crimes Enforcement Network (2000), "The SAR activity review – trends, tips and issues", FINCEN Report.

Financial Industry Regulatory Authority (2018), "Technology based innovations for regulatory compliance in the securities industry", FINRA Report.

Hayble-Gomes, E. (2022), "The use of predictive modeling to identify relevant features for suspicious activity reporting", *Journal of Money Laundering Control*, doi: 10.1108/JMLC-02-2022-0034.

Herbert, G. (2022), "Global developments in trade-based money laundering", Institute of Development Studies, Emerging Issues Report No. 55.

Institute of International Finance (2018), *Machine Learning in anti-Money Laundering*, IIF Summary Report.

International Telecommunications Union (2017), "Digital financial services ecosystem", *ITU-T Focus Group Digital Financial Services Report*, International Telecommunications Union.

Javelin Strategy and Research (2022), "Identity fraud study: the virtual battleground", Javelin Report, available at: https://javelinstrategy.com/2022-Identity-fraud-scams-report (accessed 1 March 2023).

Juniper Research (2018), *How Regtech is Revolutionising Compliance*, Juniper Research White Paper.

Juniper Research (2022), "Regtech: emerging trends, regulatory impact and market forecasts 2022-2026", Juniper Research Report.

KPMG (2018), "There's a revolution coming: embracing the challenge of RegTech 3.0", KPMG Report.

Lagerwaard, P. (2023), "Financial surveillance and the role of the financial intelligence unit (FIU) in The Netherlands", *Journal of Money Laundering Control*, Vol. 26 No. 7, pp. 63-84.

Lange, C. (1921), "Nobel lecture", 13 December 1921, available at: www.nobelprize.org/prizes/peace/1921/lange/lecture/ (accessed 1 March 2023).

Lee, C. (2006), "Constitutional cash: are banks guilty of racial profiling in implementing the United States patriot act?", *Michigan Journal of Race and Law*, Vol. 11, pp. 557-604.

LexisNexis Risk Solutions (2016), *Uncover the True Cost of anti-Money Laundering and KYC Compliance*, LexisNexis Brief.

Liu, H.-W., Lin, C.-F. and Chen, Y.-J. (2019), "Beyond state v loomis: artificial intelligence, government algorithmization and accountability", *International Journal of Law and Information Technology*, Vol. 27 No. 2, pp. 122-141.

McCarthy, J. (2022), "The regulation of RegTech and SupTech in finance: ensuring consistency in principle and in practice", *Journal of Financial Regulation and Compliance*, doi: 10.1108/JFRC-01-2022-0004.

McKinsey and Company (2022), "The fight against money laundering: machine learning is a game changer", Insights, available at: www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer (accessed 1 March 2023)

OECD (2019), "Recommendation of the council on artificial intelligence", OECD Recommendation OECD/LEGAL/0449.

Partington, R. (2017), "Banks trimming compliance staff as $321 billion in fines abate", *Bloomberg*.

Pavlidis, G. (2021), "Financial action task force and the fight against money laundering and the financing of terrorism: quo vadimus?", *Journal of Financial Crime*, Vol. 28 No. 3, pp. 765-773.

Pavlidis, G. (2022), "Europe in the digital age: regulating digital finance without suffocating innovation", *Law Innovation and Technology*, Vol. 13 No. 2, pp. 464-477.

Renda, A. (2022), "Beyond the brussels effect: leveraging digital regulations for strategic autonomy, policy brief, strategic autonomy project, foundation for European progressive studies, friedrich-ebertstiftung", Fondation Jean-Jaurès.

Saravalle, E. (2022), "Recasting sanctions and anti-money laundering: from national security to unilateral financial regulation", Columbia Business Law Review, Vol. 2022 No. 1, available at: https://journals.library.columbia.edu/index.php/CBLR/article/view/9987 (accessed 1 March 2023).

Scott, B. (2020), "OFAC sanctions compliance: insights from recent enforcement actions", *Journal of Financial Compliance*, Vol. 3 No. 3, pp. 247-254.

Stone, P., *et al.* (2016), "Artificial intelligence and life in 2030 – one hundred year study on artificial intelligence", Stanford University Study Panel, available at: http://ai100.stanford.edu/2016-report (accessed 1 March 2023).

U.S. Department of the Treasury (2023), "Financial crimes enforcement network: congressional budget justification and annual performance plan and report FY2023", Report.

Walshe, J. and Cropper, T. (2018), "Should you be banking on RegTech?", *Journal of Securities Operations and Custody*, Vol. 10 No. 2, pp. 167-175.

Yeoh, P. (2019), "Artificial intelligence: accelerator or panacea for financial crime?", *Journal of Financial Crime*, Vol. 26 No. 2, pp. 634-646.

Corresponding author
Georgios Pavlidis can be contacted at: g.pavlidis@nup.ac.cy