Georgios Pavlidis

Regulatory Technology (RegTech) and the Fight against Money Laundering: Mapping the Challenges

NUP Jean Monnet Working Paper Series

1/2021

With the support of the Erasmus+ Programme of the European Union

Neapolis University Pafos

The NUP Jean Monnet Working Paper Series can be found at:

https://www.nup.ac.cy/jean-monnet-chair/working-papers/

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP JEAN MONNET WORKING PAPER NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

RegTech and the Fight against Money Laundering: Mapping the Challenges

Abstract

In recent years, an alarming increase in the compliance costs and risks associated with anti-money laundering (AML) and combating the financing of terrorism has spurred fast-growing investment in Regulatory technology (RegTech) by financial institutions, big tech companies and RegTech start-ups. To improve compliance with Know-Your-Customer (KYC) standards, financial institutions explore RegTech solutions, such as remote customer identification, electronic identity authentication, blockchain and machine learning. In the area of transaction monitoring, the use of RegTech will allow financial institutions to promptly process large amounts of payment data on a real-time basis, analyse patterns of customer behaviour and quickly and more accurately identify suspicious activities. We argue that the choice to invest in RegTech can pay off in the long-term, on the condition that the RegTech tools are applied with the necessary robustness and consistency, and in accordance with Financial Action Task Force (FATF) standards.

Keywords:

Regulatory technology (RegTech), Money Laundering, Compliance, Know-Your-Customer (KYC), Suspicious Activity Report (SAR), Financial Action Task Force (FATF), Machine Learning, Big Data

1. Introduction

Regulatory technology (RegTech) is a fast-growing element of financial technology (FinTech) innovation; its vast potential qualifies it as an up-and-coming revolution.[1] RegTech promises to enhance regulatory processes and the delivery of regulatory requirements through the utilisation of information technology (IT) innovation, in particular artificial intelligence (AI), machine learning and Big Data. [2] Evidently, the development of RegTech has to adhere to and keep pace with requirements in the area of Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT), as stated in international conventions and Financial Action Task Force (FATF) standards, and as incorporated in domestic law. This adaptation is far from easy; it requires a continuous and constructive dialogue between policy makers, the financial industry and RegTech developers. This paper aims to map key challenges and opportunities in the RegTech area from an AML/CFT perspective, thus contributing to this ongoing dialogue.

The moment for such a discussion is very opportune, since AML/CFT compliance has been complicated due to the ever-increasing volume of cross-border transactions and the growing sophistication of techniques for money laundering and terrorism financing, as evidenced in numerous FATF reports in the last two decades.[3] Simultaneously, the volume of suspicious activity reports (SARs) that authorities receive and have to investigate has increased; for example, in the United States (US), the number of SARs filed to the Financial Crimes Enforcement Network (FinCEN) has almost doubled, i.e. from 2.7 million SARs in 2013 to 5.2 million SARs in 2018, and there are no signs that the trend is slowing down.[4] AML/CFT compliance has also been complicated by the evolving regulatory environment, the diversification of normative sources of AML/CFT standards at the national, European Union (EU) and international levels and the proliferation of targeted sanctions that regimes enforce against individuals and entities. In the US, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers an increasing number of sanctions programs targeting foreign countries, regimes, companies and individuals suspected of terrorism, drug trafficking, money laundering, etc. Ultimately, this has placed a substantial

---

[1] KPMG, *There's a Revolution Coming: Embracing the Challenge of RegTech 3.0* (KPMG 2018).

[2] P Stone and others, 'Artificial Intelligence and Life in 2030 - One Hundred Year Study on Artificial Intelligence' (2016) Stanford University Study Panel <http://ai100.stanford.edu/2016-report> accessed 8 June 2019; E Brynjolfsson and A McAfee, 'What's Driving the Machine Learning Explosion' (2017) Harvard Business Review, 18 July 2017 <https://hbr.org/2017/07/whats-driving-the-machine-learning-explosion> accessed 8 June 2017.

[3] See among others, FATF, 'Emerging Terrorist Financing Risks' (FATF Report 2015); FATF, 'Money Laundering Using New Payment Methods' (FATF Report 2010); FATF, 'Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems' (FATF Report 2008), etc.

[4] See FinCEN Suspicious Activity Report Statistics (2019) <https://www.fincen.gov/reports/sar-stats> accessed 8 June 2019.

compliance burden on financial institutions.[5] An additional burden for financial institutions has been the gradual expansion of the scope of financial crimes in many jurisdictions, which now may cover tax evasion (e.g. UK Criminal Finances Act 2017) and bribery, sometimes with extraterritorial reach (e.g. UK Bribery Act 2010).[6]

To shield themselves against aggressive enforcement and multi-billion-dollar fines for non-compliance,[7] financial institutions have to allocate more resources and time to support their compliance teams' efforts to effectively review the massive number of alerts generated by their AML/CFT monitoring systems.[8] Consequently, financial institutions may have to spend up to four percent of their revenue on regulatory compliance.[9]

Not surprisingly, this alarming increase in costs and risks has pushed the financial industry to vigorously explore new technological solutions for the digital transformation and redesign of its approach to AML/CFT compliance.[10] In addition to investment by leading financial institutions and big tech companies, currently, there is a proliferation of RegTech start-ups proposing innovative products and solutions in the field of AML/CFT, with start-up funding reaching a record 5 billion USD in a five-year period.[11] According to some estimates, RegTech investment by financial institutions, big tech companies and RegTech start-ups is expected to reach 115 billion USD by 2023, increasing much faster than the amount spent for compliance as a whole.[12]

Nevertheless, in the absence of a common international framework for the development of RegTech solutions, it is difficult for financial institutions to choose the technological products that would best shield them against compliance risks, especially when these institutions operate in multiple jurisdictions. In this context, we argue that the development of commonly accepted standards and principles for RegTech in the AML/CFT field is urgently needed. This task has to be entrusted to the FATF, the principal international forum on AML/CFT. On a positive note, since

---

[5] See <https://www.treasury.gov/resource-center/sanctions/Pages/legal-index.aspx>

[6] Iris HY Chiu, 'A New Era in FinTech Payment Innovations? A Perspective from the Institutions and Regulation of Payment Systems' (2017) 9(2) Law, Innovation and Technology 190, 201.

[7] R Partington, 'Banks Trimming Compliance Staff as $321 Billion in Fines Abate' (*Bloomberg*, 23 March 2017)

[8] This challenge has been identified in all recent Thomson Reuters Global Cost of Compliance Surveys (2016-2018) <https://legal.thomsonreuters.com/en/insights/articles/cost-of-compliance-2018-report-your-biggest-challenges-revealed> accessed 8 June 2019.

[9] Duff & Phelps, *Global Regulatory Outlook Viewpoint* (Duff & Phelps 2017) 4; A Labbé, 'Why RegTech Must Be Regulated' (2017) International Financial Law Review 1; J Walshe, T Cropper, 'Should You Be Banking on RegTech?' 10(2) Journal of Securities Operations & Custody 167-175.

[10] LexisNexis Risk Solutions, *Uncover the True Cost of Anti-Money Laundering & KYC Compliance* (LexisNexis 2016).

[11] CBInsights, 'Regtech Startups On Pace for Record Deals, Against Backdrop of Shifting Regulatory Landscape' (Research Brief, CBInsights 2017).

[12] Juniper Research, 'How Regtech is Revolutionising Compliance' (Juniper Research White Paper 2018).

2017, the FATF has recognised the regulatory and supervisory challenges posed by RegTech, and it has supported a dialogue with the private sector as part of the FATF Private Sector Consultative Forum.[13] This is a work in progress that has already presented its first results, such as the 2017 San Jose Guiding Principles;[14] nevertheless, in light of rapid RegTech innovation, and from an AML/CFT perspective, much standard-setting work is still needed, and it is worth mapping the challenges in this field.

2. The Know-Your-Customer Requirement in the Era of RegTech

RegTech can enhance customer identification and identity management and control, which are key requirements of AML/CFT regulations.[15] The know-your-customer (KYC) requirements, set in national legislations,[16] follow international standards, in particular FATF Recommendation No. 10 and applicable provisions in international law[17] and EU-instruments.[18] According to these requirements, financial institutions, as well as persons and other entities subjected to AML/CFT regulations, must undertake customer due diligence not only when establishing business relations (onboarding), but also when carrying out transactions above a designated threshold. [19] Regardless of the thresholds, customer due diligence must also be applied when there is a suspicion of money laundering or terrorist financing, or doubts about the veracity of existing data on the customer or beneficial owner.[20] Enhanced due diligence and checks are

[13] On the FATF FinTech and RegTech Initiative and the outcomes of the events organized by FATF, see <http://www.fatf-gafi.org/fr/publications/initiativefintechregtech/documents/?hf=10&b=0&s=desc(fatf_releasedate) accessed 8 June 2019.

[14] San Jose Guiding Principles (2017) <http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-fintech-regtech-forum-may-2017.html> accessed 8 June 2019.

[15] DW Arner, DA Zetzsche, RP Buckley, JN Barberis, 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities' (2019) European Business Organization Law Review 1–26.

[16] 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.

[17] 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.

[18] See, EU Fifth Money Laundering Directive (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 156/43, 2018)

[19] Under EU law, this threshold is currently EUR 15 000 for transactions 'carried out in a single operation or in several operations which appear to be linked' or EUR 10 000 for cash payments from or to persons trading in goods; article 11, Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 141/73, 2015.

[20] Ibid, article 11(e)(f).

required for Politically Exposed Persons (PEPs) and persons and entities targeted by sanctions.[21]

To improve compliance with relevant KYC standards, financial institutions explore RegTech solutions, such as remote customer identification, electronic identity authentication, blockchain and machine learning. More specifically:

i) Remote customer identification can facilitate identity verification, thus accelerating the processing of applications for accounts, loans, etc. For example, the German Federal Financial Supervisory Authority (BaFin), in cooperation with market participants, has already developed video identification procedures and requirements (e.g. encryption standards for video-chat applications) intended for persons and entities within the meaning of the German Money Laundering Act.[22] In this context, we argue that a paradigm shift is necessary, so the financial sector can fully benefit from these types of technologies: national legislation, EU law and the FATF have to recognise that remote customer due diligence can no longer be considered to be high risk, by default.[23]

ii) Electronic identity authentication (e-KYC) is a more complex tool. It is already employed in some jurisdictions, with 22 countries already giving financial institutions access to government-run digital ID systems for KYC purposes.[24] For example, customers in India can allow financial institutions to capture their fingerprints with biometric fingerprint readers and match them with data stored with the Unique Identification Authority of India, a government-run central database that stores individuals' names, addresses, dates of birth, fingerprints, photographs, iris scans, etc.[25] The advantages of e-KYC have been recognised at the EU level, where an Expert Group on e-KYC has been established, bringing together AML/CTF experts from the public and private sector in order to recommend best practices for remote onboarding in accordance with AML/CTF requirements.[26] A FATF Guidance is currently being developed on the use of digital identity to conduct customer due diligence in accordance with FATF Recommendation No. 10.[27]

iii) Going one step further from e-KYC, financial institutions could use blockchain-enabled KYC to improve customer data verification. The idea is to use

[21] FATF, 'Politically Exposed Persons' (FATF Guidance, June 2013) 6.
[22] Circular 3/2017 of 10 April 2017; section 2 (1) no. 2c Geldwäschegesetz – GwG.
[23] On this issue see Minutes of the 2nd meeting of the EU Expert Group on Electronic Identification and Remote Know-Your-Customer Processes (Brussels, 10 July 2018); see Commission Decision setting up the Commission expert group on electronic identification and remote KnowYour-Customer processes, C(2017) 8405.
[24] International Telecommunications Union, 'Digital Financial Services Ecosystem' (ITU-T Focus Group Digital Financial Services, 2017) 68.
[25] FATF, 'Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence' (FATF Guidance, November 2017) 14
[26] Commission Decision (n 23).
[27] FATF, 'Business Bulletin' (FATF Private Sector Consultative Forum, May 2019) 3.

a public digital ledger to securely store the customer's KYC-compliant documents. Thus, blockchain-enabled KYC could help validate the verification of customer data across financial institutions. This would reduce duplication and delays at onboarding, since there would be no need to repeatedly provide the same information to different financial services providers.[28] Blockchain-enabled KYC could also significantly improve customers' protection against identity fraud and account takeover. It would also facilitate the process of updating personal information across multiple accounts and institutions, as any institution using blockchain-enabled KYC would be privy to such updates.[29]

iv) RegTech tools can help financial institutions effectively detect instances of identity fraud at onboarding. This is particularly important in view of the increase in the number of cases of identity fraud, with the number of victims reaching a record high of 16.7 million in the US alone.[30] To deal with this risk, specialised tools are currently available for to detect the customers' native language based on an analysis of written communications, to detect tampered digital images or video sources (e.g. facial morphing) and to capture of the customers' GPS data on mobile phones to assess geographical money laundering risks.[31] Other behavioural data, such as the way a person enters a password, could also be analysed and used as second-factor authentication methods.[32]

v) Last, but not least, RegTech tools using automated and self-learning algorithms can significantly improve and expedite KYC by helping a compliance team better assess the risks associated with a customer. In particular, KYC algorithms can use data from various sources and in different languages (numerical data, documents, oral communications, biometric facial recognition, company and beneficial ownership registers, sanctions and other watch lists, PEP Registers, etc.) to improve KYC in cases of PEPs and their entourage, persons engaging in identity fraud, persons and entities targeted by sanctions, etc.[33] Evidently, regardless of the tools used, under AML/CFT regulations, financial

---

[28] E Maguire, 'Blockchain KYC utility' (KPMG, 2018) <https://home.kpmg/xx/en/home/insights/2018/02/blockchain-kyc-utility-fs.html> accessed 8 June 2019.

[29] B Weinberg, 'Blockchain and KYC: Know Your Customer Better' (Blockchain insights, 16 January 2019) <https://openledger.info/insights/blockchain-kyc/> accessed 8 June 2019.

[30] 'Identity Fraud: Fraud Enters a New Era of Complexity' (Javelin Report, 2018) <https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity> accessed 8 June 2019.

[31] European Supervisory Authorities, 'Opinion on the Use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process' (JC 2017 81, 23 January 2018) par. 19-22.

[32] D Arner and others, 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities' (2019) 20 European Business Organization Law Review 55–80, 60.

[33] S Breslow and others, 'The New Frontier in Anti–Money Laundering' (McKinsey & Company, November 2017).

institutions and their compliance teams are responsible for the implementation of KYC requirements (see Section 4).

3. Using RegTech Tools for Transaction Monitoring and Reporting

In the area of transaction monitoring, the use of RegTech is even more promising, since it would allow financial institutions to promptly process large amounts of transaction data on a real-time basis, analyse patterns of customer behaviour and quickly and more accurately identify suspicious activities, in accordance with the relevant reporting requirements of each jurisdiction.

National legislation and international standards, in particular FATF Recommendation No. 20, impose on financial institutions the obligation to identify, detect and report suspicious transactions to the national financial intelligence unit (FIU), such as the FinCEN in the US.[34] Compliance with the applicable requirements on suspicious activities reporting is a significant issue for financial institutions, since failure to comply may result in criminal or administrative sanctions. To effectively mitigate compliance risks, financial institutions explore promising RegTech solutions, in particular machine learning, increased automation and Big Data, to improve transaction monitoring and reporting processes. More specifically:

i) RegTech tools allow for reconfigurations in order to promptly adapt to changes in AML/CFT requirements. Adaptation would, otherwise, require too much time and effort to deploy, given the rapid growth of regulatory activity, worldwide, with an estimated 500% increase in regulatory changes after the global financial crisis.[35] It has been correctly pointed out that creating regulations in the form of machine-readable code would improve the work of regulators, enabling them to avoid 'duplication, redundancy and potential contradictions in the rules';[36] it would also enhance the work of RegTech developers and, ultimately, financial institutions.[37] In this context, the development of uniform data formats, compatible application interfaces and machine-readable monitoring mechanisms is also crucial.[38]

ii) Furthermore, new tools for monitoring transactions and identifying anomalies should be developed, based on machine learning. For example, adaptive behavioural analytics build baseline behavioural profiles for customers by monitoring their transactions over time, so fraudulent or suspicious activities can

[34] See Title 31 of the Code of Federal Regulations sec. 1010.320.
[35] MEDICI, RegTech Report 2018: Executive Summary, MEDICI Report vol. 3 (2018) 4.
[36] B Monterio, 'RegTech Is in Fashion' (2017) Strategic Finance 50-54, 53.
[37] Institute of International Finance, 'RegTech in Financial Services: Technology Solutions for Compliance and Reporting' (IFI Report, March 2016) 19.
[38] D Yang, M Li, 'Evolutionary Approaches and the Construction of Technology-Driven Regulations' (2018) 54 Emerging Markets Finance & Trade 3256–3271, 3257.

be identified almost instantly.[39] Statistical processes and self-learning algorithms can be used to predict the likelihood that a transaction is fraudulent or part of a money laundering scheme, without resorting to human subjective analysis.

iii) Machine learning and increased automation of the monitoring and reporting processes could limit false alerts and the alert fatigue that results from an overwhelming backlog of unreviewed alerts. The accumulation of unreviewed alerts is often due to 'inadequate manpower, inexperienced AML staff, improperly tuned scenarios, etc'.[40] It is estimated that RegTech tools can reduce false-positives, currently representing 90% of alerts, to less than 50%, thereby reducing the workload of compliance teams.[41] Not surprisingly, financial institutions already increasingly use machine learning to reduce false positive rates in monitoring results and increase the overall efficiency of AML defences.[42]

iv) RegTech tools can combine customer information and real-time transaction data with data from multiple and heterogeneous datasets, including e-mails, invoices, bills of lading, insurance certificates, regulatory data and other external data. Shared tools may also be utilised, in compliance with any data privacy legislation, pooling data from various financial firms to better trace transactions and the movement of funds across the financial industry.[43] Big Data tools can improve the effectiveness and lower the costs of aggregating, analysing and exchanging large amount of data, ultimately helping to ensure compliance with AML/CFT regulations. The challenge is to identify weak-signal patterns in huge volumes of data from various sources, with hundreds of transactions coming in per second. For example, Big Data analytics and algorithms may allow us to detect if unit prices in a series of transactions diverge from established international thresholds, and identify attempts to overstate or understate the

[39] D Excell, 'Using Adaptive Behavioral Analytics to Detect Fraud' (Risk Management Monitor, November 1, 2018) <https://www.riskmanagementmonitor.com/using-adaptive-behavioral-analytics-to-detect-fraud/> accessed 8 June 2019.

[40] Terence Ho, 'AML/CFT Transaction Monitoring: Alert-Based Monitoring vs Case-Based Monitoring' (ACAMS 2017) <http://files.acams.org/pdfs/2017/AML_CFT_Transaction_Monitoring_T.Ho.pdf?_ga=2.135415219.30217162.1554997585-675356344.1554997585> accessed 8 June 2019.

[41] S Breslow and others (n 33).

[42] Institute of International Finance, 'Machine Learning in Anti-Money Laundering' (IIF Summary Report, October 2018). For the purposes of the IIF study, machine learning techniques included: '1. The use of cross-validation to model relationships in the data; 2. A primary goal of out-of-sample predictive performance using regularization; 3. A significant degree of automation in the model development process; 4. Applicability to very large volumes of data, in some cases including unstructured data sources'.

[43] Financial Industry Regulatory Authority, 'Technology Based Innovations for Regulatory Compliance in the Securities Industry' (FINRA 2018) 4-5.

quantity of traded goods relative to payments, thus identifying trade-based money laundering schemes.[44]

4. Mapping Challenges and Opportunities

Financial globalisation and the expansion of financial institutions across sectors and jurisdictions have increased the regulatory challenges faced by market participants, as regulators increasingly adopt aggressive enforcement strategies and expect more from the financial sector in the fight against money laundering and financing of terrorism.[45] The dynamic and complex nature of money laundering and terrorist financing, which reflects the evolution and complexity of financial products and services, demands that market participants be extremely vigilant and adaptive to changing conditions.[46] In this environment, it is challenging to ensure effective risk management and AML/CFT compliance, which the development of powerful IT tools promises to address. To realise this promise, financial institutions have to first invest in and upgrade or replace obsolete automated systems and platforms; however, this transition can be costly.[47]

Regardless of the means and technological tools used, firms, and their compliance teams, remain responsible for the application of customer due diligence under applicable AML/CFT regimes. It has been correctly noted that RegTech tools should supplement, not replace, traditional KYC mechanisms and transaction reporting, for 'innovation [...] if ill understood or badly applied, may weaken firms' ML/TF safeguards and subsequently, undermine the integrity of the markets in which they operate'.[48] The scope of RegTech tools and the automation of processes allow compliance teams and a firm's staff to focus on analysis of information, rather than struggling to gather and organise large volumes of information from various sources. Financial institutions do not, in fact, aim at eliminating the human element of AML/CFT; rather, they seek to free up resources and shift them to higher risk cases, supporting their analysts with RegTech tools.[49] Moreover, since the role of AI in criminal acts, from cyber-attacks to financial crime, is very likely to increase in the future, before long it will become imperative

---

[44] Bankers Association for Finance and Trade, 'Combating Trade Based Money Laundering: Rethinking the Approach' (BAFT Report 2017) 5; FATF, 'Trade-Based Money Laundering' (FATF Report 2006) 24;

[45] E McCormick, 'Catching Up to RegTech' (Bank Director, 2nd Quarter 2018) 36.

[46] S Gao and others, 'Knowledge-Based Anti-Money Laundering: A Software Agent Bank Application' (2009) 13(2) Journal of Knowledge Management 63-75.

[47] E Barreto, 'Financial Firms Seek RegTech to Cut Regulatory Chores, Fight Crime' (Reuters 2016) <https://www.reuters.com/article/us-asia-fintech-regulations/financial-firms-seek-regtech-to-cut-regulatory-chores-fight-crime-idUSKBN1360UQ> accessed 8 June 2019.

[48] European Supervisory Authorities, 'Opinion on the Use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process' (JC 2017 81, 23 January 2018) par. 6.

[49] Institute of International Finance (n 42) 3.

that compliance teams must be equipped with powerful RegTech to counter the new threats.[50]

Nevertheless, we have to consider that, if promising new tools, such as algorithms and Big Data, are not properly designed and deployed in the criminal justice context or in other contexts of public authority, there is a risk of undermining 'due process, equal protection and transparency'.[51] Inevitably, the use of RegTech tools, especially Big Data, would be a source of new risks in the area of cyber resilience, secure data transmission and data privacy. Therefore, it is imperative that financial institutions and RegTech companies ensure data quality, consistency, and completeness, to 'reduce flawed automated decision-making or profiling'.[52] It is also imperative that RegTech solutions, especially complex algorithmic systems, incorporate safeguards against inherently subjective data inputs and selection bias.[53]

RegTech will be a challenge for the financial industry, as well as governments that have to remedy their 'long suffered shortages in IT skills and literacy' and develop tools, such as those used to deal with Big Data.[54] Clearly, policymakers need to develop scientifically grounded and informed regulatory approaches and principles to handle the risks associated with RegTech, such as the risk of an adversarial AI capable of altering financial data during data transfers. [55] Evidently, a collaborative framework and close engagement between governments and the private sector is needed to foster a shared understanding of RegTech developments.[56]

---

[50] P Yeoh, 'Artificial Intelligence: Accelerator or Panacea for Financial Crime?' (2019) Journal of Financial Crime (Earlycite) <https://doi.org/10.1108/JFC-08-2018-0077> accessed 8 June 2019.

[51] Han-Wei Liu, Ching-Fu Lin, Yu-Jie Chen, 'Beyond State v Loomis: Artificial Intelligence, Government Algorithmization and Accountability' (2019) 27(2) International Journal of Law and Information Technology 122–141.

[52] See Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the Purposes of Regulation 2016/679' (17/EN WP 251 rev 01, 2018) 11–12.

[53] See Executive Office of the President, 'Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights' (Executive Office of the President 2016) 8; as this report points out, if data is 'collected only from the individuals that own smartphones, then the system's results may be more accurate for wealthier populations with higher concentrations of smart phones and less accurate in poorer areas where smart-phone concentrations are lower'.

[54] DH Shin, 'Demystifying Big Data: Anatomy of Big Data Developmental Process' (2016) 40 Telecommunications Policy 837-54; D Yang and M Li, 'Evolutionary Approaches and the Construction of Technology-Driven Regulations' (2018) 54 Emerging Markets Finance & Trade 3256–3271.

[55] A Lauterbach, 'Artificial Intelligence and Policy: Quo Vadis?' (2019) Digital Policy, Regulation and Governance (Earlycite) <https://doi.org/10.1108/DPRG-09-2018-0054> accessed 8 June 2019.

[56] San Jose Principle No 2.

5. Concluding Remarks

If all these challenges are properly addressed, RegTech solutions have the capacity to revolutionise the fight against money laundering and the financing of terrorism. It has been shown that RegTech can provide promising solutions in the area of customer identification to comply with KYC requirements, as well as in the area of transactions monitoring to identify suspicious activities, promptly and accurately. RegTech can lower regulatory risk, reduce compliance costs and increase the efficiency of AML/CFT procedures; therefore, a financial firm's decision to invest in RegTech tools and infrastructure can pay off in the long-term, if the appropriate RegTech tools and methodologies are applied with the necessary robustness and consistency and in compliance with FATF standards.