2025 | 2

ELFR

EUROPEAN LAW AND FINANCE REVIEW

Rivista Semestrale
(Giugno/Dicembre
2025)

ISSN: 2975-0911

La sede della Redazione è presso l'Università San Raffaele di Roma,
Via di Val Cannuta n. 247, Roma, 00166

www.europeanlawandfinancereview.com

REGOLE PER LA VALUTAZIONE DEI CONTRIBUTI

Al fine di assicurare uno *standard* elevato della qualità scientifica dei contributi pubblicati, nel rispetto dei principi di integrità della ricerca scientifica, la Rivista adotta un modello di revisione dei manoscritti proposti per la pubblicazione che contempla il referaggio tra pari a doppio cieco (*double blind peer review*).

I contributi inviati alla Rivista sono oggetto di esame da parte due valutatori individuati all'interno di un elenco, periodicamente aggiornato, di Professori ordinari, associati e ricercatori in materie giuridiche.

Per ulteriori informazioni relative alla procedura di valutazione, si rinvia al Codice Etico pubblicato sul sito della Rivista.

EMAIL
info@europeanlawandfinancereview.com

NEXT GENERATION AML SOLUTIONS: AN ANALYSIS OF AI-BASED TOOLS *VIS-À-VIS* THE REFORM OF THE EUROPEAN AML INSTITUTIONAL AND SUBSTANTIVE ARCHITECTURE

Andrea Minto – Yaron Hazan

Next generation AML solutions: an analysis of ai-based tools *vis-à-vis* the reform of the european aml institutional and substantive architecture*

(Soluzioni AML di nuova generazione: un'analisi degli strumenti basati sull'intelligenza artificiale nel contesto della riforma organica antiriciclaggio europea)

Andrea Minto**

Full Professor of Law and Regulation of Financial Markets at Ca' Foscari University of Venice and at the University of Stavanger – School of Business and Law

Yaron Hazan**

Vice President, Regulatory Affairs at ThetaRay and Advisory Board Member at the AI APAC Institute

ABSTRACT [En]:

Despite massive policy efforts, persistent deficiencies, inconsistent enforcement, and regulatory fragmentation continue to undermine the effectiveness of anti-money laundering and counter-terrorist financing ("AML/CTF") frameworks. This article investigates the fascinating intersection between technological innovation and AML regulation, arguing that emerging technologies, particularly artificial intelligence ("AI") and machine learning ("ML"), have become both a catalyst for regulatory change and a potential remedy for systemic shortcomings. The article first examines the structural ineffectiveness of current AML regimes. It then analyzes the evolution of international standards and EU reforms, focusing on the 2024 "AML package," which includes the creation of the Anti-Money Laundering Authority ("AMLA") and the so-called AML single rulebook (the AML Regulation or "AMLR"). Against this backdrop, the article explores whether and how emerging technologies could aid obliged entities in fulfilling increasingly demanding customer due diligence and transaction monitoring obligations. By integrating insights from the growing literature on RegTech and conducting a comparative regulatory and standard-setting assessment, the study conceptualizes AI not merely as a compliance tool but as a transformative organizational instrument. It argues in fact that in light of the growing emphasis on efficient and risk-sensitive AML internal governance, AI-driven solutions are likely to become a de facto requirement for financial institutions to meet their AML obligations. Ultimately, the article contends that the future of AML effectiveness will hinge on reconciling technological capability with normative legitimacy, characterizing AI-based solutions as an essential component of an efficient and adequate AML internal governance.

Keywords: AML/CFT; Artificial Intelligence; Compliance; Internal Governance, AMLA/AMLR

ABSTRACT [IT]:

Nonostante i massicci sforzi dei *policy makers*, le persistenti carenze, l'applicazione incoerente e la frammentazione normativa continuano a minare l'efficacia dei quadri normativi antiriciclaggio ("AML/CTF"). Questo articolo indaga l'affascinante intersezione tra innovazione tecnologica e regolamentazione AML, sostenendo che le tecnologie emergenti, in particolare l'intelligenza artificiale ('AI') e il machine learning ("ML"), sono diventate sia un catalizzatore per il cambiamento normativo sia un potenziale rimedio alle riscontrate carenze. L'articolo esamina innanzitutto l'inefficacia strutturale degli attuali regimi AML. Analizza poi l'evoluzione degli standard internazionali e delle riforme dell'UE, concentrandosi sul "pacchetto AML" del 2024, che include la creazione dell'Autorità antiriciclaggio (AMLA) e il cosiddetto regolamento AML (AMLR). In questo contesto, l'articolo esplora se e in che modo le tecnologie emergenti possono aiutare i soggetti obbligati ad adempiere agli obblighi sempre più stringenti di due diligence sui clienti e di monitoraggio delle transazioni. Integrando le conoscenze tratte dalla crescente letteratura sul RegTech e in virtù di un'analisi comparativa, lo studio sostiene che le soluzioni basate sull'IA come una componente essenziale di una governance interna AML efficiente e adeguata.

Parole chiave: AML/CFT; Intelligenza Artificiale; Compliance; Governance Interna, AMLA/AMLR.

1. INTRODUCTION

Over the last 20 years the fight against money laundering and terrorist financing has been one of the major priorities in the agenda of policy-makers and regulators world-wide. Anti-money laundering and counter-terrorist financing (AML/CTF) legislation has in fact expanded in scope and complexity, with the European Union (EU) progressively consolidating its framework through successive legislative acts. Yet, despite these efforts, high-profile scandals - spanning from the HSBC and Danske Bank cases to the more recent failures involving major international crypto-asset service providers - have revealed deep structural deficiencies. These cases demonstrate a persistent misalignment between regulatory expectations, supervisory practices, and the

compliance standards of financial institutions. Indeed, despite two decades of incremental reforms, the AML regime remains characterized by inefficiency, inconsistent enforcement, and a lack of clarity regarding what "effective compliance" entails.

Against this backdrop, one of the most persistent points of contention relating to AML/CTF legislation concerns the breadth of its regulatory scope. However tightly drawn the AML "regulatory net" may be, criminal actors have repeatedly demonstrated ability in circumventing it, exploiting loopholes and structural blind spots inherent in any regulatory framework that, by its nature, can never be entirely comprehensive[1]. This tension is particularly pronounced in view of the accelerated pace of financial innovation, which has introduced new market participants, digital service offerings, and technologically enabled business models.[2]

The exponential increase in digitalization has reconfigured the financial ecosystem in ways that legislators and supervisors struggle to address[3]. At the European level, financial innovation has not only prompted policymakers to take stock of the current market reconfiguration but has also served as a catalyst for comprehensive reform - reshaping both institutional design and substantive regulatory requirements[4].

---

*Il contributo è stato approvato da revisori.

** This research has been funded by the ThetaRay Fellowship.
I am indebted to ThetaRay staff for the productive exchange of ideas in particular during the event and seminar held in Athens and Madrid on 22 January and 27 May 2025 respectively.

Although this article is the result of a joint reflection, par. 1, 3, 5, 6, 7, 8 and 9 can be primarily attributed to Andrea Minto, with the remaining sections primarily attributable to Yaron Hazan.

[1] On the opportunities for regulatory arbitrage, see e.g. M. THIEMANN, T. TRÖGER, *The Case for a Normatively Charged Approach to Regulating Shadow Banking - Multipolar Regulatory Dialogues as a Means to Detect Tail Risks and Preclude Regulatory Arbitrage*, in *SAFE Working Paper No. 260*, 2020; T. VLAD, A. FARRANT, *The Efficiency of Regulatory Arbitrage* 181(1), in *Public Choice*, 2019, 141; A. RILES, *Managing Regulatory Arbitrage: A Conflict of Laws Approach* 47(1) in *Cornell International Law Journal*, 2014, 147; M. HEIKKI, *The Problem of Regulatory Arbitrage: A Transaction Cost Economics Perspective* 15(2), in *Regulation & Governance*, 2019, 388; V. FLEISCHER, *Regulatory Arbitrage* 89, in *Texas Law Review*, 2010, 227.

[2] See, e.g., INTERNATIONAL MONETARY FUND, *Elements of Effective Policies for Crypto Assets*, in *IMF Policy Papers*, February 2023; see also, among others, BASEL COMMITTEE on BANKING SUPERVISION, *Prudential Treatment of Crypto-asset Exposures*, in *Consultative Document*, June 2022; FINANCIAL STABILITY BOARD, *International Regulation of Crypto-asset Activities: A Proposed Framework*, 11 October 2022; FINANCIAL STABILITY BOARD, *Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications*, June 2019; EUROPEAN CENTRAL BANK, *Crypto-Assets Task Force, Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments Market Infrastructures,* in *ECB Occasional Paper Series* no. 223, 2019. In the legal scholarship, see, e.g., I. H-Y CHIU, *A New Era in Fintech Payment Innovations? A Perspective from the Institutions and Regulation of Payment Systems* 9, in *Law, Innovation and Technology*, 2017, 190 2017; I. H-Y CHIU, *Regulating the Crypto Economy: Business Transformations and Financialisation*, in *Oxford, Hart Publishing*, 2021; I. H-Y CHIU & G. DEIPENBROCK (eds.), *Routledge Handbook of Financial Technology and Law*, London, Routledge, 2021; J. MADIR (ed.), *FinTech Law and Regulation*, Elgar Financial Law and Practice Series, Cheltenham, Edward Elgar Publishing, 2021.

[3] R. POL, *Anti-money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It* 3(1), in *Policy Design and Practice*, 2020, 73; S. BROWN, *Cryptocurrency and Criminality: The Bitcoin Opportunity* 89(4), in *The Police Journal: Theory, Practice and Principles*, 2016, 327; W. BOLT, V. LUBBERSEN and P. WIERTS, *Getting the Balance Right: Crypto, Stablecoin and Central Bank Digital Currency* 16(1), in *Journal of Payments Strategy & Systems*, 2022, 39; R. COELHO, J. FISHMAN and D. GARCIA OCAMPO, *Supervising Cryptoassets for Anti-Money Laundering*, in *Bank for International Settlements, Financial Stability Institute*, 2021; T. FRICK, *Virtual and Cryptocurrencies—Regulatory and Anti-Money Laundering Approaches in the European Union and in Switzerland* 20(1), in *Era Forum*, 2019, 99.

[4] As better illustrated over the next sections of the article, the EU legislators set in motion a true reform of the institutional and substantive architecture of AML supervision and legislation by means of the so called "*AML package*". The AML package branches out into four specific legislative trajectories resulting in Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024); Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and

The rapid growth of the crypto-asset industry illustrates these dynamics particularly well. In recent years, mainstream adoption has accelerated as individuals, businesses, and financial institutions have become increasingly engaged with the crypto ecosystem. While distributed ledger technology (DLT) undeniably offers substantial opportunities, it simultaneously raises complex questions regarding emerging AML risks and the adequacy of existing safeguards[5].

Yet, not only does technology raise new AML risks, it also provides innovative tools and measures to cope with such risks. In fact, technology itself is becoming a driver of compliance transformation. Artificial intelligence (AI), machine learning (ML), and advanced analytics have emerged as potential "next-generation" solutions to chronic AML challenges, such as high false-positive rates, inefficient resource allocation, and the difficulty of detecting sophisticated laundering schemes. These technologies promise to enhance anomaly detection, automate monitoring, and enable financial institutions to process vast datasets at speeds that far exceed human capabilities. Unsurprisingly, policymakers have begun to explore the potential advantages as well as the challenges of the adoption of emerging technologies for AML compliance. International standard-setting bodies such as the Financial Action Task Force ("FATF") have published guidance on the responsible use of AI, emphasizing transparency, accountability, and proportionality. Similarly, the OECD and national regulators have issued principles for trustworthy AI.

In this perspective, the European Union amounts to a very interesting case study, as it can be said to sit at the forefront of this intersection between AML reform and AI governance. In fact, the EU legislators have recently enacted two pieces of legislation that comprehensively deal with both such areas: on the one hand, the so-called "AML package" puts in motion an unprecedented reform which includes the creation of a centralized Anti-Money Laundering Authority (the "AMLA") and the harmonization of substantive obligations across Member States. On the other hand, the EU Artificial Intelligence Act ("AI Act") introduces a horizontal regulatory framework for AI technologies, categorizing AI systems according to their risk profiles and imposing stringent obligations on high-risk applications. The interaction of these two legal regimes raises significant

Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (OJ L, 2024/1620, 19.6.2024); Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (OJ L, 2024/1640, 19.6.2024); and Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

[5] The technologically dynamic nature of the crypto-asset ecosystem has exposed the limitations of traditional AML/CTF measures which have struggled to keep pace with the sector's rapid evolution. In fact, anonymizing technologies enabling products such as privacy coins (e.g., tokens that employ advanced cryptographic techniques to obscure transaction details.) and tumblers or mixers made transaction monitoring more challenging, undermining both financial transparency and Know Your Customer (KYC) obligations. Additionally, the cross-border nature of crypto businesses – resulting in service providers frequently operating across jurisdictions that have divergent levels of regulatory maturity - increased the risk of regulatory arbitrage. See FINANCIAL ACTION TASK FORCE (FATF), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020, 7–8, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf; A. NARAYANAN et al., *Bitcoin and Cryptocurrency Technologies*, in *Princeton: Princeton University Press*, 2016, 140–143.

doctrinal and practical questions as to whether and how AI-enabled AML tools could remedy long-standing deficiencies in compliance and supervision.

This dual evolution underscores a fundamental paradox: the same technological advances that may hold the key to more effective AML compliance also raise new concerns regarding legal certainty, due process, explainability, and accountability. Furthermore, the AI Act may simultaneously constrain their development or deployment, thereby introducing potential frictions between technological innovation and regulatory safeguards. Accordingly, this paper situates itself at the intersection of technology law, financial regulation, and compliance. It analyzes the capacity of AI-based AML tools to serve as a legally and operationally sound response to the existing deficiencies, while also considering the normative boundaries imposed by EU law. More specifically, it aims to examine whether and how AI can bridge the persistent implementation gap between regulatory expectations and business practices, or whether its adoption will generate a new layer of legal uncertainty. Ultimately, this article advances the argument that emerging technologies constitute an inevitable organizational instrument which - as adapted to size, complexity, and risk profile - *all* credit institutions will likely be required to adopt in order to fulfil their obligations to establish effective and proportionate AML internal governance mechanisms. Not only are banks required to allocate compliance resources in proportion to identified risk (in line with the risk-based approach and principle of proportionality), but they also have to implement such resources in a manner that is efficient and consistent with the technical and technological progress.

The remainder of this article is structured as follows: chapter 2 examines the shortcomings of the current AML regulatory and supervisory frameworks. Chapter 3 offers an overview of the recent guidelines and best practices developed by the international standard setters, as well as by the European Union by means of the recent AML package. The analysis continues in Chapter 4 by providing a literature review of the opportunities and threats of technology advancement in finance.

2. INEFFECTIVENESS OF AML REGULATORY AND SUPERVISORY FRAMEWORKS

Saying that the current framework for AML and CTF is ineffective may sound like a problematic statement, but official organizations support this claim: Europol estimates that only about 2% of criminal proceeds are frozen and 1% confiscated in the EU.[6]

The outcome of the fight against financial crimes is expected to be measured in prevention, detection, investigation and eventually seizure of illicit assets and bringing criminals to jail.

The 'path to success' is dependent on various stages that must be performed by: financial institutions as the private sector gate keeper, Financial Intelligence Units ("FIUs") as the receptor of the identified cases, Law Enforcement Agencies ("LEA") as the investigator to find the evidence for a crime, district attorneys' offices to

[6] Report from the commission to the European parliament and the council, Asset recovery and confiscation: Ensuring that crime does not pay, June2, 2020, page 1, introduction.

bring the cases to court, and eventually judges to take the final decision "the verdict."

It is essential to understand that all participants invest efforts and budget to maximize the full defense net but significant structural gaps remain.

The FATF stated that nearly all (97%) of 120 assessed countries have low to moderate effectiveness rating for preventing money laundering and terrorist financing.[7]

FIUs traditionally report that only around 10% of cases reported to LEA lead to action[8].For example, in the Netherlands, during 2024, out of 3,484,373 reports to the FIU, 118,408 were identified as suspicious -less than 3.5% [9] ; in France Tracfin report on their actionable Sars around 5%[10] during 2023.

Banks traditionally report low conversion stats from alert to SAR, Wolfsberg Group refer in their Suspicious Activity Monitoring ("SAM") report, 2024 to the entirety of the problem:

Alert-to-SAR conversion rates, both in terms of poor outcomes and their limited reflection of effectiveness, often fail to capture genuinely suspicious activity.According to the 2022 Germany FIU report, only 15% of SARs were investigated by law enforcement authorities, and 95% of forwarded cases ended without prosecution.

The conclusion of ineffectiveness is coming from FIUs, Europol, Banks, TM vendors and anyone involved in this important challenge.

The root cause for lack of effectiveness can be traced to several structural factors:

A. Understanding and acknowledging the responsibility of FIs in the fight against financial crimes has not always been straightforward. Several cases in the early 2000s showed that banks did not always understand their role in defending humanity against financial crimes. Circumvention and repeated weaknesses were identified in several regulatory reviews by the US regulators focusing on HSBC, which led to the 1.9 B USD fine, a DPA and threat of losing license and potentially even sending senior officials to jail.

B. A lack of practical understanding of how to implement the necessary controls to address the regulatory expectation also led to attempts to adapt fraud detection controls for AML purposes, creating miss-alignment between Know Your Customer processes and ongoing activity monitoring, a focus on the wrong risks, and ultimately poor outcomes. The Wolfsberg Group's 2019 statement even calls banks to stop redundant activities.[11]

C. Technology was also part of the failure. Banks often tried to use unsuitable solutions. In order to effectively cover the complexity of AML risks, FIs needed sophistication that at the early 2000s was not market ready, hence, the tools implemented as common practice were not fit for purpose.

3. OVERVIEW OF GUIDELINES AND BEST PRACTICES CONCERNING AML

[7] Report on the state of effectiveness and compliance with the FATF standards, 2022, page 7.
[8] Report by Europol, *From suspicious to action*, 2017, page 29.
[9] *Annual review, FIU Netherlands, 2024,* p. 7.
[10] *Tracfin, press release,* July 31, 2024
[11] The Wolfsberg Group - Statement on Effectiveness, 2019.

DEVELOPED BY THE INTERNATIONAL STANDARD SETTERS

Over the past decade and a half, international standard setters have intensified their efforts to refine the global AML/CTF architecture. While the *Financial Action Task Force* ("FATF") remains the cornerstone of this transnational regime, many other bodies at the international and national level echoed the need to increase the effectiveness of AML/CTF regulatory frameworks, in terms of both supervision and substantive requirements.

Such "wake-up call" resulted in a wide set of soft-law acts, ranging from the documents issued by the Basel Committee on Banking Supervision ("BCBS"), the Wolfsberg Group, the OECD, and the Egmont Group of Financial Intelligence Units. Taken together, these sources articulate a complex fabric of "global standards" that both shaped hard law and set benchmarks for supervisory expectations. Yet, despite this proliferation of normative frameworks, repeated evaluations and thematic reviews revealed that AML regimes across jurisdictions suffered from endemic weaknesses. The literature and official reports converge on a central insight: compliance has expanded dramatically in its formal dimension, but its *effectiveness* remains uncertain.

Against this backdrop, the identified factors branch out into several axes (the so-called "effectiveness gap"[12], the beneficial ownership transparency, the limits and paradoxes of the risk-based approach, transaction monitoring and the quality of STRs…). In this context, transaction monitoring most certainly amounts to be one of the most visible pressure points in the global AML/CTF regime in that it reveals a structural tension between regulatory expectations and institutional capacity. This became particularly true after the 2012 revision of the FATF Recommendations, and its subsequent methodology, which placed the *risk-based approach* ("RBA") at the heart of transaction monitoring, requiring financial institutions to calibrate systems proportionately to the nature and magnitude of the risks they face[13]. Yet in practice, mutual evaluation reports and thematic reviews demonstrate that obligated entities, under supervisory pressure, often default to over-reporting rather than risk-sensitive detection. The system thereby drifts into what the Wolfsberg Group has characterized as "process-driven compliance," producing suspicious transaction reports (STRs) of limited investigative utility.[14]

This problem is particularly acute in correspondent banking and other cross-border business models. By design, in fact, correspondent institutions process vast volumes of transactions on behalf of respondent banks, with only fragmentary knowledge of the underlying customers. FATF has long recognized this "opacity problem": FATF Recommendation 13 and its interpretative notes underscore the vulnerability of correspondent banking to misuse precisely because the correspondent institution cannot apply full customer due diligence.[15]

---

[12] Perhaps the most salient critique emerging from the last two FATF evaluation cycles (2013–2025) is the "effectiveness gap". Many jurisdictions can demonstrate *technical compliance* with the forty recommendations, but this has not translated into demonstrable reductions in money laundering or improved capacity to trace, freeze, and confiscate illicit assets. FATF's *Report on the State of Effectiveness and Compliance* (2025) underscores that countries often build extensive legislative frameworks while failing to produce concrete outcomes across the eleven Immediate Outcomes, particularly in relation to supervision, preventive measures, and asset recovery. The result is a paradoxical regime in which rules proliferate, but the real-world impact of those rules remains opaque.

[13] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, 2012.

[14] WOLFSBERG GROUP, *Statement on Effectiveness* (2019); *Statement on Monitoring for Suspicious Activity*, 2024.

[15] FATF, Recommendation 13 and Interpretative Note, 2012.

Yet, paradoxically, supervisory expectations increasingly require correspondents to implement transaction monitoring frameworks capable of detecting sophisticated laundering typologies across opaque flows. The Wolfsberg Principles on Correspondent Banking illustrate this paradox: while they provide industry-driven guidance on minimum due diligence, they simultaneously acknowledge that correspondents must rely to a significant extent on respondents' controls, creating a structural asymmetry of information.[16]

The consequences of this imbalance are evident. In doctrinal terms, transaction monitoring obligations in the correspondent context expose regulated entities to a form of *impossible compliance*. Institutions are required to monitor risks that, by their very nature, remain concealed. The Basel Committee on Banking Supervision has highlighted that governance in this area is often deficient: boards and senior management frequently fail to integrate transaction monitoring into enterprise-wide risk frameworks, resulting in fragmented oversight and inadequate control testing[17]. Meanwhile, the Egmont Group's work on financial intelligence units (FIUs) emphasizes that cross-border information exchange remains slow and inconsistent, depriving correspondents of the contextual intelligence necessary to make monitoring systems effective.[18] In the absence of reliable cross-border data, monitoring becomes a blunt instrument, generating high false-positive rates, straining institutional resources, and producing STRs that law enforcement agencies themselves often deem of limited value.

These shortcomings are not merely operational but doctrinal. The risk-based approach is intended to ensure proportionality and flexibility, yet in the transaction monitoring space it often functions as a legal fiction. Institutions, particularly those operating in cross-border contexts, face obligations that are disproportionate to their informational and technical capacities. This structural imbalance undermines both the principle of proportionality and the legitimacy of AML law itself, as compliance becomes an exercise in defensive reporting rather than risk management. In doctrinal terms, the regime reflects what might be called *normative overreach*: the imposition of duties without a realistic possibility of their fulfillment.

In line with such developments, the same pressing need to restructure the architecture of AML legislation and supervision was expressed by EU policy-makers. Indeed, the European Commission in two important Communications between 2019[19] and 2020[20], set out the measures needed to ensure a comprehensive EU policy on preventing money laundering and countering the financing of terrorism (AML/CFT). "*These include better implementation of existing rules, a more detailed and harmonised rulebook, high-quality and consistent supervision, including by conferring specific supervisory tasks to an EU body, interconnection of centralised bank account registries and a stronger mechanism to coordinate and support the work of the Financial Intelligence Units (FIUs)*".

The policy plan of the European Commission resulted in the "AML package", a reform that dealt with

---

[16] WOLFSBERG GROUP, *Correspondent Banking Principles* (2014, revised 2022).

[17] BASEL COMMITTEE, *Sound Management of Risks related to ML/TF* (2017).

[18] EGMONT GROUP, *Principles for Information Exchange* (2025); *FIU Effectiveness in Asset Recovery* (2025).

[19] See EUROPEAN COMMISSION, *Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework*, 24 July 2019.

[20] See EUROPEAN COMMISSION, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, 7 May 2020.

both the institutional and the substantive dimensions of the AML architecture. Such reform will be analyzed in chapter 5.

4. OPPORTUNITIES AND THREATS OF TECHNOLOGY IN AN EVOLVING LANDSCAPE: LITERATURE REVIEW

Technology is perceived as a growth driver, according to economic models developed following the 1956 "Solow-Swan Model", named after the 2 researchers who brought to the economic science the perception that maximizing capital and human resources can drive growth at a certain pace but technology could significantly increase productivity. Technology in the 21st century has already become an inherent part of everything we do, the basis for work, science, business and human interaction.

Technology and various IT infrastructure have been part of global banking for decades. The SWIFT infrastructure was created in 1973 and started operating in 1977 to enable messaging between banks and has, ever since, reshaped the global economy.

When it comes to inherent challenges in the fight against Money Laundering, Technology for AML and financial crime fighting also contributed to the problem. Initially systems were siloed and designed to solve a specific challenge in a complex FI-customer relationship and bank-to-bank relationships. The landscape of Transaction Monitoring has been perceived as a failure, inefficient and ineffective for decades. One study focused on operational risk management examined AML in a bank as a case study and found that rule based scenarios resulted in only 2% reporting[21]. The bank tried to apply machine learning and other methods to avoid wasting so much time on too many redundant alerts, but the key question to be asked is should these alerts be generated in the first place?

The root cause for this inefficiency is mainly found in the approach, tools supporting AML risk management were, and in most cases, still are, rule based.

Since 2018, many regulators and thought leaders call for using machine learning and AI in the financial crime prevention and detection. Some regulators also conducted experiments and initiated projects with the Private sector to review the potential of technology for a new era of effectiveness.

These documents reflect the understanding of these organizations that Machine Learning and AI can bring more success to the AML controls:

January 2018: The EBA European Banking Authority and ESMA European Securities and Markets Authority published an opinion on the use of innovative solutions by credit and financial institutions in the customer Due Diligence process. Clause 14 (pages 5-6), outlines the advantages of such solutions, including large-scale data analytics, improved investigation focus, high-volume processing, streamlined decision making and reduced false alerts.

[21] Operating the boundary system: A case study of Anti- Money Laundering risk management in a bank, 2025, page 15.

December 2018: Joint statement by FINCEN and other US regulators encouraging innovative industry approaches to AML compliance, suggesting AI can contribute both to efficiency as well as effectiveness.

2019: Banca D'Italia published a document exploring the opportunities in Suptech applications in Anti Money Laundering, starting with the basic need to analyze larger volumes of data and explaining the potential advantages in several new tech methods. This document shares some real life examples of actual use cases by supervisors and FIUs that leverage the tech capabilities.

2020: EBF, The European Banking Federation, published a document "Lifting the spell of dirty money", calling for a more effective EU framework., The call for change is focused on getting better outcomes and the use of AI is mentioned several times as big potential to improve expert decisions and judgment (p. 33) and to increase the ability to identify patterns in criminal activity (p. 35).

2021: FATF published two documents, one for the private sector and one for the public sector, together with Egmont group, directing FIUs challenges and opportunities.

This trend is reflected in numerous additional publications, and in the past 3 years the move to AI and even generative AI impacted almost every aspect of life, while Transaction Monitoring and Financial Crime Risk Management remain "Rule-based" in most Financial operations.

A good example of the magnitude of this change is how smart tools can improve the detection of complex patterns in the use case of Correspondent Banking. Correspondent Banking has always been a challenge for financial crime risk management. As described above, the banks have to provide services to other banks and rely on their controls. The Wolfsberg group, composed of leading global banks, was established for that purpose, and developed the "Wolfsberg Questionnaire" as the standard for banks' due diligence.

These questionnaires focus on a long list of risk indicators and support the decision on whether to onboard a financial institution or not. If the decision is to open a service account to the applicant, the bank assigns an appropriate risk rating. What does this rating serve? How does this rating impact the ongoing monitoring? Can banks really identify risks posed by a related Financial Institution during the business relationship?

At the same time, Fintechs and Crypto based service providers added the pressure on banks to a Straight Through Processing of payments and services.

The challenge in that case is even greater: banks must not only be able to identify risks, but they must do so with increasing speed.

The ability to identify and understand risks in a complex cross border activity is not easy, currently, the facts that are monitored are uni-dimensional and there is little insight to be gained from such a narrow view.

For example, if a non-customer generates a high volume of transactions, from a specific jurisdiction, sent in certain currency to a certain destination, processed by a "Correspondent Bank" ("CB"), the CB has very limited visibility into the underlying activity.

This raises the question of what, in practice, a correspondent bank can identify?

In a rules based; approach, each data field/parameter is evaluated against predefined thresholds. In

financial crime related scenarios, there are several data elements that combine together to a "behavior." Can the CB set a rule per each parameter? What could be learned and understood if each rule was breached? Should each alert be investigated separately? That is the current status in most banks.

This is a clear example of where AI can provide value:: instead of relying on"uni-dimensional" analysis, moving to a "multi-dimensional" one.

The ability, in Correspondent Banking, to focus on "Pseudo customers" (i.e., entities treated analytically as customers despite not being direct clients) can mitigate some of the knowledge gaps that exist in such cross-border activity.

Instead of focusing on predefined scenarios, simple and unidimensional, that are known to any bad guy who wants to bypass the system, looking at a combination of behavioral risk indicators enables a wider view of facts.

Such AI based detection can also fulfil the common requirements from banks in accordance with the due diligence practices defined through the "Wolfsberg Questionnaire."

It does so by utilizing the information collected at a specific point in time and detecting the behavior against the expected activity on an ongoing basis.

The risk posed by banks and other FIs can also be covered, as AI-based models can focus both on the pseudo-customer and the financial institutions involved.

This is a simple example of a complex challenge that seemed almost impossible to solve, that can be simplified and managed both efficiently and effectively.

The potential scenarios that could be related to a prohibited activity through CB are relevant to relationships between financial institutions, such as undeclared "nesting" and to the actual predicate offenses that Anti Money Laundering is aiming to slow down/detect/prevent.

The move from rules that are focussed on predefined scenarios, that are financial related by nature, such as geography, products, services and industry, to AI based patterns, can also enable focus on actual suspicious activity that is potentially indicating a crime, for example, human trafficking detection or terrorist financing detection.

The changes described here can, and should, be the focus of AML requirements, controls and best practices.

Responsible AI standards are key for AI to be used in the financial system, In the recent years, many regulators published guidance documents related with the use of AI in the Financial system, Monetary Authority of Singapore published the "FEAT" principles in 2018, Fairness, Ethics, Accountability and Transparency, staging that AI and machine learning tools could be biased and rely on past knowledge that is not ideal, unfair and mis judging, such bias could damage the decisions when recruiting an employee or offering services to customers.

The MAS provides in this document a direction that there should be a differentiated approach to fighting financial crime, the principle of transparency even includes a statement that:

"For example, the AIDA Firm uses AIDA models for fraud detection and to identify possible "red flags". Given materiality considerations and concerns of model manipulation or exploitation, an AIDA Firm decides not to share about the AIDA model used, or provide explanations relating to this area".

This shows one important perception: while the criteria for assessing the fit of AI model are clear, different use cases should be considered by their nature, financial institution is asked to reveal the use of AI that drives specific selection of services or products to customers, but, at the same time, is not expected to reveal to all, including bad guys, how the AI is used for financial crime detection.

The struggle between "conflicting values" is not new. GDPR requirements are strict when it comes to personal data, yet at the same time, public interest and security are at least as important values and the path between conflicting objectives should be carefully selected.

In order to feel confidence when applying AI solutions to Financial Crime Risk Management, the question is not limited to the values, it is also about the translation of the values into principles, and practical methodologies.

Responsible AI in Fighting Crime - Principles and Best Practices.

Financial regulators published many guidance documents for responsible use of AI solutions, some of them, such as the French regulator, ACPR, already shared with the financial industry several documents with an evolving understanding and expectations.

From 2018, the "FEAT" principals document mentioned above, the regulators focused on several criteria to assess the reliability of AI solutions, The DNB, DeNederlandschebank published on July 2019 a guidance document listing the following principals[22]: Soundness and skills were added to the initial "FEAT" principles, in order to understand these principles, the relevant risks when using AI and the expected controls, DNB provided the following guidance:

- Soundness-risk of experiencing systemic mistakes should be mitigated by experts' involvement, the choice of the solution should meet the explainability and simplicity criteria, alignment with organization's AI policy;
- AI is implemented to serve specific tasks, all employees involved from production to the board level should understand the risks and limitations of the organizational AI systems. Audit, Risk and Compliance teams should be trained to understand AI related risks and challenges.
- In June 2020, ACPR published a document focused on the "Governance of Artificial Intelligence in Finance"- Inthis document, Explainability and Governance of AI are the key focus areas and AML is one of the main use cases tested, The document mention the difference between interpretability "the degree to which an observer can understand the cause of a decision" and explainability is broken to model creation and post model creation phases:

[22] See General principles for the use of AI in the financial sector, DNB, 2019, Pages 34-39,

- Pre-model explanatory methods mainly refer to which data sources were used and why
- Documentation of data sets and decisions
- Explainable feature engineering relying on experts involvement
- Post model creation explanatory approach should be defined at early stage of model adaption, to enable planning of embedding AI into the business process.

"Lastly, explainable modelling is not very suitable for audit, all the more so when the predictive model is only available as a black box, without a documentation of the algorithm itself".

Explainability, according with ACPR guidance should be tested considering the following criteria:

Accurate, Comprehensive, Comprehensible, Concise, Actionable, Robust, Reusable.[23]

All these criteria should explain how the model operates and why the model took specific decisions. As per the governance part, the document emphasizes the following requirements:

Operational procedures, segregation of duties, risk recognition and assessment, integration in business process, role of AI, engineering methodology and user interaction with AI.

As many Financial regulators acknowledged the advantages in using AI for AML controls, these publications were critical for FIs to understand what would be considered as responsible implementation of AI into business processes.

These guidance documents between 2018-2023 evolved to the magnitude of laws in various countries that defined the requirements, guidelines and restrictions around the use of AI technology in accordance with the risks identified in the past 6 years. Such legislation includes: CANADA, Artificial Intelligence and data act, second reading was completed in April 2023. US, Executive order 14110 on the safe secured and trust worthy developments and use of Artificial Intelligence. Brazil, Bill No. 2338/2023 that defines responsibilities and penalties for AI developers, Approved in December 2024. UK, Pro innovation approach to AI regulation, August 2023. South Korea, The AI framework act, December 2024.

The wind of change is emphasized through all these regulatory documents, on the one hand a clear understanding that AI is part of modern life and modern society, on the other hand, the needs for safeguards and governance. These laws, in the use case of AI solutions for AML controls in the financial industry, enable progress and advanced use of AI while clarifying the responsibility of all entities involved, adapters and providers.

These laws and guidelines, including the AI Act, can and should be translated into clear best practices for AI adaptation. The principles have not changed: Human involvement, Accountability, Explainability, Safety, Fairness and Transparency.

Similar to any risk management practice, these should be measured and managed with a clear understanding of probability for the risk and the potential impact.

[23] See L. DUPONT, O. FLICHE, S. YANG, ACPR guidance: "Governance for artificial intelligence in finance" June 2020, by: Fintech-Innovation Hub, ACPR,various clauses re explainability and Governance.

Per the AML use case, it should not be too complex, responsible AI should be explainable, based on facts and involve experts prior to any decision.

AI has already become an embedded tool in the hands of bad actors, using it wisely can mitigate some of the risks posed to society by these bad actors.

5. TECHNOLOGY AS A DRIVER FOR REGULATORY CHANGE (1): THE "AML PACKAGE" IN THE EUROPEAN UNION.

As already emphasized, the evolution of EU AML legislation has proceeded along two principal trajectories. First, the regulatory architecture has incrementally broadened its *scope of application* in an effort to encompass an ever-wider range of economic operators and professional actors whose activities may serve as leverage points for the detection and prevention of financial crime (the "obliged entities"). Second, the AML framework has consistently sought to reinforce the *substantive effectiveness* of transaction monitoring mechanisms by refining the checks, controls, and due diligence obligations imposed upon obliged entities.

A decisive inflection point in this legislative trajectory occurred with Directive 2001/97/EC (the second AML directive, or "AMLD2"), adopted a decade after the first Anti-Money Laundering Directive ("AMLD1"). While AMLD1 had confined its scope to "credit and financial institutions," AMLD2 represented a genuine paradigm shift by extending the subjective reach of AML obligations to a considerably broader array of entities and professionals. From that juncture onward - through successive updates of the AML framework and culminating in the recent Regulation (EU) 2024/1624 (the "AMLR") - the circle of obliged entities has continued to expand, reflecting the Union's commitment to a progressively comprehensive and risk-based approach to the prevention of money laundering and related financial crimes.

In the wake of unprecedented scandals[24], EU policy makers were called upon to increase the effectiveness of the current AML architecture by rolling out a complete institutional and substantive overhaul [25]. On 20 July 2021, in fact, the European Commission triggered the law-making process and presented its proposal to reform the anti-money laundering and counter-terrorism system, which consists of a series of measures, namely: (i) the 6th Anti-Money Laundering Directive [26]; (ii) the regulation establishing a European *Anti-Money Laundering Authority* or "AMLA"[27]; (iii) the regulation containing certain directly applicable AML/CFT rules, including in relation to customer due diligence and beneficial ownership; (iv) a revision of the Regulation (EU) No 2015/847 on funds transfers for the purpose of tracking crypto assets transfers (the only measure that has so far been taken by means of Regulation (EU) 2023/1113, as discussed above).

The first measure to be taken was the above-mentioned Travel Rule Regulation by means of Regulation (EU)

[24] Namely, the "Danske bank case" stands out as, that, amounts to be one of the biggest AML scandals in Europe, in terms of overall magnitude, with over 200 billion euro in ML transactions. See, e.g., A. MINTO, N. RASMUSSEN, *Approaching the Danske Bank Scandal in a "Tragedy of the Commons" Perspective: Implications for Anti-Money Laundering Institutional Design and Regulatory Reforms in Europe* 19(2) European Company and Financial Law Review 305 (2022).

[25] See in particular Communication from the Commission to the European Parliament and the Council *Towards Better Implementation of the EU's Anti-Money Laundering and Countering the Financing of Terrorism Framework*, COM/2019/360 final, 24 July 2019; Communication from the Commission on an *Action Plan for a Comprehensive Union Policy on Preventing Money Laundering And Terrorist Financing,* 2020/C 164/06 (so called "Commission AML Action Plan", C/2020/2800), 13 May 2020.

[26] COM (2021) 423 *final.*

[27] COM (2021) 421 *final.*

2023/1113. On 19 June 2024, the remaining three of the four building-blocks of the so called "AML package" – the AML Regulation (Regulation (EU) 2024/1624, the "AMLR"), the Regulation establishing the Anti-Money Laundering Authority (Regulation (EU) 2024/ 1620, the "AMLAR") and the sixth AML Directive (Directive (EU) 2024/1640, the "AMLD6") - have been published on the Official Journal of the EU, setting in motion a true paradigmatic shift in the institutional[28] and substantive[29] architecture of the field.

The recent overhaul of the AML regulatory framework has been driven, amongst other things, by the quest to counter the new AML risks associated with digitalization and technology advancement. The measure underlying the AML package in fact "*refine the existing EU regulatory framework, adapting it to new and emerging challenges related to technological innovation*…" [30].

6. TECHNOLOGY AS A DRIVER FOR REGULATORY CHANGE (2): THE "AI ACT"

As new technologies disrupt established social, economic, and institutional arrangements, law is compelled to reshape its instruments, concepts, and methodologies in order to account for the resulting transformations. We just showed that technological innovation functioned as a catalyst for legal evolution in the AML ambit. Along the same lines, the accelerating diffusion of AI prompted EU policy makers to develop novel regulatory frameworks to acknowledge the emerging technologies and make sure to preserve (fundamental) rights and their responsible and proper adoption, while sustaining innovation and competitiveness.

The enactment of Regulation (EU) 2024/1689 (the Artificial Intelligence Act, or "AI Act") constitutes a paradigmatic instance of this phenomenon. It illustrates how technological change operates not merely as a passive object of regulation but as an active *driver of regulatory transformation*. The AI Act reflects an attempt by the EU to translate technological complexity into legal form, thereby establishing a comprehensive framework capable of addressing both the risks and the societal potential of AI.

As recital 1 states, in fact, the AI Act aims to "*improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and*

[28] Indeed, a new EU agency, the Anti-Money Laundering Authority ("AMLA") has been established with the responsibility to manage the AML/CFT supervisory system.

[29] In looking at the AML requirements, it is worth emphasizing the paradigm shift that the EU legislator made by moving from a directive-based legislation to a regulation-based framework: since 1991 (when the first AML directive was enacted), and after other four acts of such nature, the decision to abandon the instrument of the directive is a much welcome, and a much needed, step forward in the direction of ensuring a consistent implementation of the AML requirements across countries (namely, customer due diligence, data retention and reporting of suspicious transactions). This holds particularly true in relation to financial markets, that are by their very nature global and thus inherently cross-border.

[30] These measures aim to refine "*the current EU regulatory framework,* adapting it *to new and emerging challenges related to technological innovation, such as virtual currencies, the increased integration of financial flows in the single market and the global nature of terrorist organisations. These proposals will help create a much more coherent framework to facilitate compliance of operators subject to AML/CFT rules, in particular those operating across borders*": those the words of the European Commission used in the Press Release, *Defeating Financial Crime: Commission Reviews Rules Against Money Laundering and Terrorist Financing* (20 July 2021), available at https://ec.europa.eu/commission/presscorner/detail/it/ip_21_3690.

trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation".

According to art. 3(1), n.1, "AI system" is defined as "*a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*".

Central to the AI Act's architecture is the risk-based approach, a regulatory philosophy that - like the approach that characterizes the AML framework, *mutatis mutandis* - seeks to calibrate legal obligations according to the potential risks that AI systems pose to fundamental rights, safety, and societal interests ([31]).

In this perspective, in fact, the AI Act develops a risk-based approach in order to introduce a proportionate and effective set of binding rules for AI systems. Such an approach, in fact, aims to "*tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain unacceptable AI practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems*" (see recital 26 AI Act). In this perspective, the regulation sets out a four-tiered taxonomy of risk, articulated in Articles 5 to 7. This structure reflects a graded intervention model designed to align the intensity of regulatory oversight with the potential severity of harm.

(a) Unacceptable Risk. Certain uses of AI are prohibited outright on the ground that they contravene fundamental values or pose disproportionate risks to human dignity and autonomy. These include systems involving social scoring by public authorities, manipulative subliminal techniques, or biometric identification for real-time surveillance, subject to narrow exceptions. This category embodies the *precautionary dimension* of the EU's regulatory philosophy, reflecting a willingness to ban technologies whose risks are deemed inherently incompatible with fundamental rights.

(b) High Risk. The *high-risk* category constitutes the core of the AI Act's regulatory apparatus. Pursuant to Article 6, systems falling within certain critical areas—such as employment, education, law enforcement, migration, and essential private services—are subject to extensive obligations. Providers of high-risk systems must conduct *ex ante conformity assessments*, ensure data governance and documentation, implement quality

[31] For a critical analysis of the AI Act's risk-based approach see, e.g., M. EBERS, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act,* in *European Journal of Risk Regulation*, 2025;16(2):684-703; J. CHAMBERLAIN, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective,* in *European Journal of Risk Regulation*, 2023;14(1):1-13. doi:10.1017/err.2022.38; L. FLORIDI, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, June 1, 2021, available at SSRN: https://ssrn.com/abstract=3873273 or http://dx.doi.org/10.2139/ssrn.3873273; EDWARDS and VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, May 23, 2017, in *Duke Law & Technology Review* 18, 2017, Available at SSRN: https://ssrn.com/abstract=2972855. or http://dx.doi.org/10.2139/ssrn.2972855.

management systems, and facilitate post-market monitoring. The obligations codified in Title III thus transform AI compliance into an ongoing process rather than a one-off certification event.

(c) Limited and Minimal Risk. AI systems deemed to present *limited* risks are subject primarily to transparency obligations—for instance, informing users that they are interacting with an AI system.

(d) Minimal Risk.

For *minimal-risk* systems, no specific obligations are imposed beyond adherence to general principles and voluntary codes of conduct. This residual category aims to preserve regulatory space for innovation and experimentation while maintaining an overarching framework of accountability.

This taxonomy illustrates the Union's preference for *graduated regulation*, balancing the imperatives of innovation and risk mitigation through differential legal intensity.

7. THE KEY DEVELOPMENT OF THE EU AML LEGISLATION AND THE INCREASED LEVEL OF SOPHISTICATION OF AML COMPLIANCE/AML OBLIGATIONS

Far from constituting a mere exercise in legislative replication, the AMLR materially advances and refines the framework established under the AMLD4 with respect to the substantive content of AML obligations. Within this broader reform agenda, one of the most significant areas of regulatory innovation concerns *customer due diligence* ("CDD"). The AMLR fundamentally restructures the CDD regime, both expanding and recalibrating the obligations originally articulated in AMLD4.

Specifically, the AMLR replaces the previous fourfold set of due diligence obligations with a more extensive and demanding framework comprising ten distinct activities, thereby altering not merely the scope but also the nature of CDD itself. This transformation introduces novel elements, such as explicit obligations related to sanctions compliance, which were previously absent from the AMLD4 framework[32]. Furthermore, the AMLR revises the *temporal and conditional triggers* for conducting due diligence, redefining the circumstances under which obligated entities must initiate CDD procedures.

According to art. 13 AMLD4, in fact, customer due diligence is formed by four specific activities. The four activities that make up the customer due diligence are: i) the identification of the customer and verification of the customer's identity on the basis of documents, data or information obtained from a reliable and independent source; ii) the identification of the beneficial owner, taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer; iii) the assessment and, as appropriate,

[32] Indeed see art. 20 AMLR that, amongst other activities, requires obliged entities to verify " whether the customer or the beneficial owners are subject to targeted financial sanctions, and, in the case of a customer or party to a legal arrangement who is a legal entity, whether natural or legal persons subject to targeted financial sanctions control the legal entity or have more than 50 % of the proprietary rights of that legal entity or majority interest in it, whether individually or collectively" (see art. 20(1)(d)).

obtainment of the information on the purpose and intended nature of the business relationship; and iv) the ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date (see art. 13, par. 1, lett. a), b), c), d), respectively) [33].

With reference to the scope of application, art. 11 AMLD4 enumerates the cases in which obligated parties are required to perform the activities described above. Specifically, the provision stipulates that customer due diligence applies:

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction that:

(i) amounts to EUR 15.000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

(ii) constitutes a transfer of funds exceeding EUR 1.000;

(c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked [34].

In addition to these cases, obliged entities are required to always carry out customer due diligence when:

(a) there is suspicion of money laundering or terrorist financing; or

(b) there is doubt about the veracity or adequacy of data previously obtained for identification purposes.

Against this backdrop, we may now move to the new CDD regime as enshrined in the AMLR.

In particular, art. 19, par. 1 of the AMLR provides that customer due diligence applies:

(a) when establishing a business relationship;

---

[33] See, e.g., MUGARURA, *Customer Due Diligence (CDD) Mandate and the Propensity of its Application as a Global AML Paradigm* 17(1), in J*ournal of Money Laundering Control* 76 (2014); CHITIMIRA, MUNEDZI, *Overview International Best Practices on Customer Due Diligence and Related Anti-Money Laundering Measures* 26(7), in J*ournal of Money Laundering Control,* 2023, 53; SHOUST, DOSTOV, *Implementing Innovative Customer Due Diligence: Proposal for Universal Model* 23(4), in J*ournal of Money Laundering Control* , 2020, 871; MULLIGAN, *Know Your Customer Regulations and the International Banking System: Towards a Self-Regulatory Regime* 22(5), in *Fordham International Law Journal*, 1998, 2372.

[34] Those cases, therefore, apply irrespective of any derogation, exemption or threshold as they always trigger the application of the customer due diligence. For the purpose of the correct fulfillment of this obligation, it makes it worthwhile to clarify - with regard to the cases referred to in Art. 11, par. 1 (a) and (b) - what is meant, respectively, by "*business relationship*" and "*occasional transaction*". While the former indicates "*a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration*" (see Art. 3, par. 3, n. 13), the occasional transaction refers to a transaction that obviously escapes the features of the business relationship, in that it lacks the duration element. However, the occasional transaction to be relevant for the application of due diligence must: i) result in a transaction of 15.000 euro or more; or ii) constitute a transfer of funds exceeding 1.000 euro.

(b) when carrying out an occasional transaction of a value of at least EUR 10 000, or the equivalent in national currency, whether that transaction is carried out in a single operation or through linked transactions […]; *(c) when participating in the creation of a legal entity, the setting up of a legal arrangement* […] *irrespective of the value of the transaction; (d) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold; (e) when there are doubts about the veracity or adequacy of previously obtained customer identification data; (f) when there are doubts as to whether the person they interact with is the customer or person authorised to act on behalf of the customer*".

By way of derogation from the general CDD rules, however, art. 19, par. 3 requires crypto-asset service providers to (a) apply customer due diligence when carrying out an occasional transaction that amounts to a value of at least EUR 1 000, or the equivalent in national currency, whether the transaction is carried out in a single operation or through linked transactions; and (b) apply at least customer due diligence measures referred to in Article 20(1), point (a), when carrying out an occasional transaction where the value is below EUR 1 000, or the equivalent in national currency, whether the transaction is carried out in a single operation or through linked transactions.

In line with the risk-based approach that informs the AML legislation, the legislator itself deemed occasional transactions in crypto assets riskier than occasional transactions with other means of payment, with the consequence of lowering the threshold for the application of CDD from EUR 10.000 to 1.000.

The manner in which CDD is articulated under Article 19 of the AMLR, when viewed against the backdrop of evolving market dynamics and the increasing sophistication of money-laundering schemes, renders compliance increasingly onerous for financial institutions to the point of challenging their capabilities. The broadened scope of CDD obligations, now encompassing a more granular assessment of risk factors, verification of beneficial ownership, and systematic integration of sanctions screening, imposes in fact considerable operational demands on banks. The convergence of stricter regulatory expectations with rapid technological and market developments exacerbates the compliance burden. Ultimately, this accentuates the tension between regulatory ambition and operational capacity, in that it raises the regulatory bar so high to make it very challenging for banks to abide by.

8. AMLR AND ARTIFICIAL INTELLIGENCE

The AMLR explicitly mentions AI. Indeed, according to art. 76(5) AMLR, in fact, "*obliged entities may adopt decisions resulting from automated processes, including profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679, or from processes involving AI systems as defined in Article 3, point (1), of Regulation (EU) 2024/1689 of the European Parliament and of the Council, provided that:*

a) the data processed by such systems is limited to data obtained pursuant to Chapter III of this Regulation;

b) any decision to enter or refuse to enter into or maintain a business relationship with a customer or to carry out or refuse to carry out an occasional transaction for a customer, or to increase or decrease the extent of the customer due diligence measures applied pursuant to Article 20 of this Regulation, is subject to meaningful human intervention to ensure the accuracy and

appropriateness of such a decision; and

c) the customer may obtain an explanation of the decision reached by the obliged entity, and may challenge that decision, except in relation to a report as referred to in Article 69 of this Regulation".

This provision however is concerned with the proper use of the data, and not with AI as a (potentially essential) component of the AML internal governance of obliged entities.

Indeed, Article 76(5) AMLR permits obliged entities to employ automated decision-making processes, including profiling and AI-driven systems, subject to the compliance with three cumulative safeguards. Each safeguard performs a distinct regulatory function aimed at ensuring that automation does not compromise the substantive and procedural guarantees embedded in the AML framework.

(1) The Data-Limitation Requirement

The first condition establishes a limitation on the categories of data that may be processed through automated systems. The provision confines permissible data to that obtained pursuant to Chapter III AMLR, which governs customer due diligence and related financial crime prevention measures. This demarcation serves two purposes. It ensures, first, that the use of automation remains tethered to the statutory objective of detecting and mitigating money-laundering risks rather than expanding into ancillary commercial uses[35]. Second, it operates as a structural safeguard against disproportionate data acquisition and the introduction of external datasets that may produce opaque or discriminatory outcomes[36]. The requirement thus reinforces the principle of purpose limitation central to EU data protection law, while aligning it with AML risk management objectives[37].

(2) The Requirement of Meaningful Human Intervention

The second condition mandates substantive human oversight over core relationship and transactional decisions. Decisions to enter, maintain, or terminate a business relationship, to execute or refuse an occasional transaction, or to adjust the level of customer due diligence measures must be subject to meaningful human intervention capable of verifying the accuracy and appropriateness of the automated output. This requirement does not endorse human involvement of a merely procedural or confirmatory nature. Rather, it requires an evaluative engagement in which the human reviewer possesses both the authority and the practical capacity to review, amend, or overturn the automated recommendation[38]. This safeguard operationalizes the broader EU

---

[35] On the need for strict necessity in data processing for AML objectives, see CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige, ECLI:EU:C:2016:970, paras 94–102.

[36] See, e.g., S. WACHTER, B. MITTELSTADT AND L. FLORIDI, *Why a Right to Explanation Does Not Exist in the GDPR*, in *International Data Privacy Law* 7(2), 2017, 76–99; M. HILDEBRANDT, *Smart Technologies and the End(s) of Law*, Edward Elgar 2015, ch 3; M. BRKAN, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the EU*, 27, in *European Journal of Law and Technology*, 2019, 287–309.

[37] On purpose limitation as a constitutional principle of EU data protection law, see CJEU, Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559, paras 175–185 and CJEU, Case C-131/12, Google Spain, ECLI:EU:C:2014:317, para 72.

[38] See Art. 14 AI Act encompassing the requirement of effective human oversight. In literature see L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to Explanation' Is Probably Not the Remedy You Are Looking Fo*r, 16 *Duke Law & Technology Review*, 18–84, at 43–48, 2017

legal principle that automated systems must not displace human responsibility in matters bearing legal or economic significance for individuals.

(3) The Right to Explanation and Contestation

The third condition affords customers the procedural right to obtain an explanation of the decision and to challenge that decision. This constitutes a due process guarantee within the AML context. It requires obliged entities to provide intelligible and sufficiently detailed information regarding the reasoning underlying the outcome, allowing the customer to contest potential inaccuracies. The only exclusion concerns decisions connected to the filing of suspicious transaction reports under Article 69 AMLR, where confidentiality is essential to the effectiveness of financial intelligence operations. This exclusion confirms that the right to explanation and contestation is calibrated to preserve both individual procedural rights and the integrity of supervisory reporting mechanisms[39].

Besides this explicit reference to AI in the AMLR, we consider it even more important (and compelling for its integration into the operational and business models), the implicit reference to it in the ambit of the set of rules concerning internal governance, as explained in the next paragraph.

9. REGTECH AND OBLIGED ENTITIES' INTERNAL GOVERNANCE: EXPLORING THE OBLIGATION TO SET UP AN EFFECTIVE ORGANIZATIONAL STRUCTURE AND ITS IMPLICATIONS VIS-À-VIS TECHNOLOGY ADVANCEMENT

Within the different trajectories the reform of the EU AML legislation branches out, a relevant one most certainly relates to the effectiveness of the internal governance measures, compliance and risk management.

Internal governance refers to the set of processes, procedures and organizational measures, as well as "*all standards and principles concerned with setting an institution's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined and clearly allocated; how reporting lines are set up and what information they convey; and how the internal control framework is organised and implemented, including accounting procedures and remuneration policies. Internal governance also encompasses sound information technology systems, outsourcing arrangements and business continuity management*"[40].

In fact, the AMLR aims to emphasize tee identification, management and mitigation of money laundering and financing of terrorism risk as an essential component of sound internal governance arrangements

[39] On the legitimacy of confidentiality exceptions in AML supervision, see CJEU, Case C-598/19, UAB "SS" v Lietuvos bankas, ECLI:EU:C:2021:800, paras 42–47 (accepting procedural limitations to preserve integrity of supervisory reporting)

[40] EBA, *Guidelines on internal governance under Directive 2013/36/EU,* 2 July 2021. On the definition of internal governance, see, e.g., VAN SETTEN, *Risk, Risk Management, and Internal Controls*, in D. Busch, G. Ferrarini, G. Van Solinge (eds.), *Governance of Financial Institutions,* in *Oxford University Press*, 2019, p. 221; HOPT, *Corporate Governance of Banks after the Financial Crisis*, in E Wymeersch, K. Hopt, and G Ferrarini (eds), in *Financial Regulation and Supervision—A Post Crisis Analysis*, Oxford University Press, 2012, p. 11 and 17; BCBS, *Guidelines. Corporate governance principles for banks*, July 2015, p. 3; MILLER, *The Law of Governance, Risk Management, and Compliance*, 2nd ed, Wolters Kluwer, 2017, 709–84; H-Y CHIU, *Regulating (from) the Inside—The Legal Framework for Internal Control,* in *Banks and Financial Institutions*, Oxford University Press, 2015; VOS. K. MORBEE, COOLS and M. Wyckaert, *A cross-sectoral analysis of corporate governance provisions*, in V. Colaert, D. Busch, T. Incalza (eds.), *European Financial Regulation. Levelling the cross-sectoral Playing field*, Hart publishing, 2019, p. 182.

and risk management frameworks. In this specific perspective, therefore, the AMLR advances the governance arrangements that credit institutions are required to have in place to ensure sound and effective risk management as provided for in this regard by the relevant requirements of the AMLD4, Directive 2013/36/EU as well as the indications in the EBA guidelines on internal governance [41].

The increased emphasis on internal governance emerges already from how the AMLR is designed.

Unlike the AMLD4, in fact, where this matter is scattered between Article 8 and then Articles 45 and 46, the AMLR shows a clear and neat structure, in that it consolidates all the relevant set of rules in Chapter II, under the heading "*internal policies, controls and procedures of obliged entities*".

The rules on internal governance thus form the first set of obligations, as enshrined in Chapter II, to be complied with. Chapter II is then divided into Sections: Section I on "*Internal Procedures, risk Assessment and staff*" and Section II concerning "*Provisions applying to groups*", thus confirming how important they are in the overall architecture of AML requirements.

The AMLR develops the current provisions of the AMLD4 in particular by adding new obligations on the management body that aim to

(i) intensify its oversight on the institution's activities;

(ii) foster the implementation of a sound risk culture; and

(iii) strengthen the risk management frameworks of institutions by including the aspect of AML risk factors.

Article 7 AMLR demonstrates the pivotal role of risk management, in that it requires credit institutions to adopt policies, controls and procedures in order to ensure compliance with the AML framework in a much more articulated and precise fashion than the corresponding Article 46 AMLD4. In particular, the internal governance should be designed as to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity, as well as to curb the risks of non-implementation and evasion of proliferation financing related targeted financial sanctions [42].

Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entity and should include: (a) the development of internal policies, controls and procedures, including risk management practices, customer due diligence, reporting, reliance and recordkeeping, the monitoring and management of compliance with such policies, controls and procedures; (b) policies, controls and procedures to identify, scrutinize and manage business relationships or occasional transactions that pose a higher or lower

---

[41] See EBA, *Guidelines on internal governance under Directive 2013/36/EU, 2 July 2021*, Executive summary: "*in recent years, internal governance issues have received increased attention from various international bodies. Their main aim has been to correct institutions' weak or superficial internal governance practices, as identified during the financial crisis. Recently, there has been a greater focus on conduct related shortcomings, including compliance with the framework to prevent money laundering and terrorist financing and activities in offshore financial centres*".

[42] The notion of "*targeted financial sanctions*" refers to "*both asset freezing and prohibitions to make funds or other assets available, directly or indirectly, for the benefit of designated persons and entities pursuant to Council Decisions adopted on the basis of Article 29 of the Treaty on European Union and Council Regulations adopted on the basis of Article 215 of the Treaty on the Functioning of the European Union*" (see art. 2 (1)(35) AMLR).

money laundering and terrorist financing risk; (c) an independent audit function to test the internal policies, controls and procedures; (d) the verification, when recruiting and assigning staff to certain tasks and functions and when appointing its agents and distributors, that those persons are of good repute, proportionate to the risks associated with the tasks and functions to be performed; (e) the internal communication of the obliged entity's internal policies, controls and procedures, including to its agents and distributors; (f) a policy on the training of employees and, where relevant, its agents and distributors with regard to measures in place in the obliged entity to comply with the AML requirements.

In designing and implementing the appropriate internal governance measures, the banks' management body has to take into account the risk variables and risk factors indicated by the AMLR[43] as well as the results of risk assessments conducted both by the Commission and by Member States.[44] The self-risk-assessment elaborated and prepared by each bank will then be made available to the supervisory authorities, according to what is already provided for in this regard by Article 8 AMLD4.

The AMLR therefore further consolidates the link between "risk assessment'" and the implementation of the "internal controls", emphasizing the functional relationship of the first (the self-assessment) phase to the second (organizational) phase. The identification of the inherent money laundering and terrorist financing risks amounts thus to a pre-condition to properly discharge the internal governance obligations, in that the policies, procedures, and internal controls will be shaped by the actual nature and level of ML risks the bank is exposed to. In carrying out their self-assessment, credit institutions are required to take into account the characteristics of their customers, the products, services or transactions offered, the countries or geographic areas concerned, and the distribution channels used (see *recital* 20 AMLR).

In this context, in a logic of graduating burdens according to exposure to the risk of money laundering,

---

[43] Risk factors are but a mere indication and they represent a non-exhaustive list of circumstances to be taken into account.

Without prejudice to this, it is worth noticing that the AMLR expands such list of risk factors, as compared to the list that the AMLD4 provides. The European Parliament has recently proposed to widen the sources and indications to be considered kept in mind much more than today. In particular, reference is made to "*relevant guidelines, recommendations and opinions issued by AMLA*", "*the conclusions drawn from past infringements of AML/CFT rules by the obliged entity in question or any connection of the obliged entity in question with a case of money laundering or terrorist financing*"; "information *from Financial Intelligence Units (FIUs) and law enforcement agencies*"; "*information obtained as part of the initial customer due diligence process and ongoing monitoring*"; "*own knowledge and professional experience*". Even, because of the principle of proportionality, the Parliament suggested inserting a new paragraph 1a in Article 8 that would enable obliged persons to interrogate additional sources and databases or professional organisations (see European Parliament, *Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, Rapporteur: Eero Heinäluoma, Damien Carême, Compromise Amendments AML Regulation, 22 March 2023).

[44] In particular, Article 7(2) AMLR identifies in a precise manner the minimum elements of the internal governance structure. Policies, controls and procedures must at least include: "*(a) the development of internal policies, controls and procedures, including risk management practices, customer due diligence, reporting, reliance and recordkeeping, the monitoring and management of compliance with such policies, controls and procedures, as well as policies in relation to the processing of personal data […]; (b) policies, controls and procedures to identify, scrutinise and manage business relationships or occasional transactions that pose a higher or lower money laundering and terrorist financing risk; (c) an independent audit function to test the internal policies, controls and procedures […]; (d) the verification, when recruiting and assigning staff to certain tasks and functions and when appointing its agents and distributors, that those persons are of good repute, proportionate to the risks associated with the tasks and functions to be performed; (e) the internal communication of the obliged entity's internal policies, controls and procedures, including to its agents and distributors; ((f) a policy on the training of employees and, where relevant, its agents and distributors with regard to measures in place in the obliged entity to comply with the requirements of this Regulation".*

the principle of proportionality and the risk-based approach ([45]) rise to guiding criteria in the fulfillment of AML obligations[46].

These are some principles that, in truth, can be said to underpin European anti-money laundering legislation since its inception in 1991, but which only through Directive 2005/60/EC and then, most importantly, Directive 2015/849/EU (the fourth anti-money laundering directive or "AMLD4") have found full realization and explicit recognition[47].

The risk-based approach, to be true, shapes and guides the conduct of both regulators and supervisors. Indeed, for one thing, Article 46(1) of the AMLD4 requires Member States to ensure that "*obliged entities take measures proportionate to their risks, nature and size so that their employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements*", for the other, Art. 48(6) states that "*when applying a risk-based approach to supervision, the competent authorities: (a) have a clear understanding of the risks of money laundering and terrorist financing present in their Member State; (b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the obliged entities; and (c) base the frequency and intensity of on-site and off-site supervision on the risk profile of obliged entities, and on the risks of money laundering and terrorist financing in that Member*".

Consistently, the aforementioned principles also inform the manner in which the customer due diligence obligation is fulfilled: it is in fact necessary for obliged entities to apply those general criteria in identifying and

---

[45]See L. DALLA PELLEGRINA, D. MASCIANDARO, *The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View*, in *Review of Law & Economics*, vol. 5, no. 2, 2009, p. 931 ss.; P. COSTANZO, *The risk-based approach to anti-money laundering and counter-terrorist financing in international and EU standards: What it is, what it entails*, in B. Unger e D. van der Linde (eds.), *Research Handbook on Money Laundering*, Edward Elgar, Cheltenham, 2013, p. 349 ss.

See also the ESAs *Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis* ("The Risk-Based Supervision Guidelines"), as amended on 16 December 2021 by the EBA. Specifically, these Guidelines require Competent Authorities to identify and assess the ML/TF risk to which their sector is exposed, and adjust the focus, intensity and frequency of supervisory actions in line with the risk-based approach. As part of an effective risk-based approach to AML/CFT supervision, Competent Authorities should have suitably qualified staff to carry out risk-based AML/CFT supervision in an informed and consistent manner. Finally, the Guidelines make it clear that the size or systemic importance of a credit or financial institution may not, by itself, be indicative of the extent to which it is exposed to ML/TF risk and that small firms that are not systemically important can nevertheless pose a high ML/TF risk.

[46]For an overview about those overarching principles, see, e.g., D. DEMETIS, D. and ANGELL, *The risk-based approach to AML: representation, paradox, and the 3rd directive*, in *Journal of Money Laundering Control*, Vol. 10 Issue No. 4, 2007, pp. 412-428; L. AI, J. BROOME and H. YAN, *Carrying out a risk-based approach to AML in China: Partial or full implementation?* in *Journal of Money Laundering Control*, 2010, 13(4): 394–404; D.S. DEMETIS, and I.O. ANGELL, *The risk-based approach to AML: Representation, paradox, and the 3rd directive*, in *Journal of Money Laundering Control*, 2007, 10(4): 412–428; D. MASCIANDARO, *Money laundering: The economics of regulation*, in *European Journal of Law and Economics*, 1999, 7(3): 225–240; L. de KOKER, *Identifying and managing low money laundering risk*, in Journal of Financial Crime, 2009, 16(4): 334–352; FATF *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures.* Paris: Financial Action Task Force, 2007; FATF, *Risk-Based Approach for the Banking Sector*, Paris: Financial Action Task Force, 2014.

[47] See H. KOSTER, *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework*, in *Journal of Money Laundering Control*, Vol. 23 No. 2, 2020, pp. 379-386. https://doi.org/10.1108/JMLC-09-2019-0073; A. MINTO, *Banks' internal governance obligations vis-à-vis money laundering risks emerging from the new technology-enabled means to transfer funds or value ("crypto assets")*, in *Journal of Money Laundering Control*, Vol. 27 No. 7, 2024, pp. 43-59. https://doi.org/10.1108/JMLC-04-2024-0068.

assessing the risks of money laundering and terrorist financing associated with customers: against such yardstick, they have to adjust the way due diligence is to be carried out. Based on the principle of the risk-based approach, therefore, the intensity and extent of the due diligence requirements are modulated according to the degree of money laundering and terrorist financing risk associated with the individual customer.

In light of the close link between the organizational obligations and the ML risk management, any entity should take into account how the tech-development could - thanks to new emerging technologies – support the fulfilment of the increasingly demanding AML obligations[48].

In such a way, the need to properly and effectively manage such ML risk will translate into organizational obligations that in turn result in the selection of the "right tools for the job". The focus is centered around *whether and how* technology advanced measures could amount to the choice that obliged entities are expected to make.

Without prejudice to the above, the integration of such new technology-enabled tools requires abiding by certain regulatory precautions regarding (i) the technology as such (e.g. the measures introduced by the AI ACT; (ii) the way data are collected, managed and processed (see art. 76(5) AMLR, and GDPR).

Indeed, despite from a governance perspective, AI could be considered to be the adequate step to take, its integration has to take into account the consequences in terms of "good data" governance as enshrined in art 76(5) AMLR. Thus, if AI adoption could be considered normatively implicitly mandated for obliged entities, yet remains constrained by data protection law and explainability obligations.

10. CONCLUDING REMARKS: RE-SHAPING THE TECHNO-LEGAL COMPLIANCE: WHEN AI COULD AMOUNT TO A MANDATORY "MEANS TO AN END"

Recent advances in technological capabilities and the evolution of market practices have contributed to a marked increase in the complexity of the financial ecosystem. This development has drawn attention to the limitations of existing AML instruments and tools and, in particular, to their capacity to achieve the regulatory objectives with which they are tasked. For regulated entities to satisfy contemporary supervisory expectations, regulatory compliance must increasingly rely on operationally viable and technology-supported means.

At the same time, the proliferation of legal sources and regulatory requirements, often pursuing different and occasionally competing objectives, has generated difficulties in interpretation and coordination. In a data-driven economic environment, financial institutions are subject to a dense layering of obligations arising from multiple regulatory regimes, including, for the purposes of the present analysis, the AMLR and the General Data Protection Regulation (GDPR). Within this context, record-keeping obligations illustrate the challenges most clearly. Such obligations have become particularly onerous amid persistent uncertainties regarding the lawful processing and retention of data, especially for institutions engaged in cross-border activities.

The analysis therefore commenced by outlining the principal challenges posed by recent market and

[48] G. PAVLIDIS, *Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era*, in J*ournal of Money Laundering Control*, 18 December 2023, 26 (7): 155–166.

technological developments, and by examining the shortcomings of the existing AML framework. It subsequently considered the regulatory responses adopted over the past decade by policymakers and standard-setting bodies. Particular attention was devoted to the European Union, where technological innovation has operated as a catalyst for regulatory adjustment. This dynamic is evidenced most notably in the ongoing AML reform package and in the adoption of the Artificial Intelligence Act.

These two legislative initiatives have evolved with the aim of reconciling regulatory expectations with the technological capacities available to market participants. Their interaction is capable of enabling obligated entities to discharge AML duties more effectively. A central element of the AML reform is the strengthening of internal AML governance, understood as the ensemble of procedures, functions, and organizational resources deployed to identify and manage money-laundering risks inherent to the institution's activities. For such governance to be considered adequate, it must incorporate technological tools commensurate with current operational realities. Consequently, nowadays, the integration of AI-based solutions in the operational business model becomes inevitable, in particular with regard to customer due diligence and transaction monitoring.