SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Artificial Intelligence in financial security: Legal challenges in Japan's AML/CFT regime and comparative insights from selected EU countries

Dawid Trela

dawidmtrela@gmail.com

https://orcid.org/0000-0001-9781-6425

Doctoral School, War Studies University, Al. gen. Chruściela "Montera" 103, 00-910 Warsaw, Poland

Abstract

This study examines the legal and regulatory challenges in deploying artificial intelligence (AI) within anti-money-laundering and counter-terrorist-financing (AML/CFT) systems in Japan (focal case) and in Germany, France, and Poland (purposive comparators). It identifies intra- and cross-jurisdictional gaps; assesses alignment with FATF Recommendations 1 and 15, the GDPR, and the EU AI Act; and distils transferable best practices. Doctrinal legal analysis and normative comparative methodology were employed, with limited functional observations where supervisory practice is documented. Sources include statutes and regulations, supervisory guidance, and case law issued from May 2015–May 2025, notably the EU AML package (Reg. (EU) 2024/1624; Dir. (EU) 2024/1640; Reg. (EU) 2024/1620) and the AI Act (Reg. (EU) 2024/1689), as well as FATF materials and national guidance (BaFin, CNIL/Tracfin, JFSA). All jurisdictions permit AI in AML/CFT, yet frameworks remain fragmented and under-specified for algorithmic decision-making. Key gaps concern liability for algorithmic outcomes; tensions between transparency/explainability and tipping-off; and safeguards for automated decisions (GDPR Art. 22). Germany/France show higher supervisory maturity (explainability, auditability, DPIA, human-in-the-loop), whereas Japan/Poland rely chiefly on general data-protection duties with limited AML/AI-specific guidance, indicating the need for governance-heavy, auditable, human-in-the-loop designs. Better coordination of the AML, AI, and data-protection regimes is required to ensure both effectiveness and fundamental-rights protection. Japan could benefit from EU practices by formalising human-in-the-loop requirements for high-impact AML decisions, mandating DPIAs, enhancing auditability/reporting for high-risk models, and expanding regulatory sandboxing. The EU should continue aligning the AI Act with the AML Regulation (via AMLA guidance), clarifying oversight, documentation, and explainability expectations for AML use cases.

Keywords:

Artificial Intelligence, explainable AI, AML/CFT, data protection, algorithmic accountability

Article info
Received: 13 August 2025
Revised: 3 November 2025
Accepted: 8 November 2025
Available online: 31 December 2025

Citation: Trela, D. (2025) 'Artificial Intelligence in financial security: Legal challenges in Japan's AML/CFT regime and comparative insights from selected EU countries', *Security and Defence Quarterly*, 52(4). doi: 10.35467/sdq/214090

http://doi.org/10.35467/sdq/214090

Introduction

Money laundering and terrorist financing represent significant threats to economic stability, public security, and the integrity of financial systems, as emphasised in numerous reports and recommendations issued by international organisations, such as the Financial Action Task Force (FATF, 2025), the Organisation for Economic Co-operation and Development (OECD, 2021), and the European Union (European Commission, 2024). It is estimated that the annual value of criminal proceeds laundered globally ranges from 2% to 5% of global GDP, amounting to approximately USD 800 billion to USD 2 trillion each year (United Nations Office on Drugs and Crime [UNODC], 2023). In Europe, according to the European Commission, the scale of money laundering may reach 1% of the EU's GDP, equivalent to around EUR 160 billion annually (European Commission, 2021). The introduction of technologically advanced solutions—most notably artificial intelligence (AI), understood here as machine-based systems that infer from input data to generate outputs (e.g., predictions, classifications, recommendations, alerts) used in AML/CFT for risk assessment, monitoring, and anomaly detection—has become imperative (Alhajeri and Alhashem, 2023, p. 286). This is in the light of constantly evolving criminal methodologies, increasingly sophisticated money laundering schemes, and the growing volume of cross-border transactions, which render traditional monitoring methods (manual reviews and static rule-based/threshold systems) virtually impossible. Throughout this article, the FATF Recommendations operate as the primary international baseline against which national approaches and AI deployments are assessed. OECD/IOSCO outputs and the EU AI Act serve as complementary reference points.

The deployment of AI significantly enhances the detection of suspicious transactions, improves the effectiveness of compliance procedures, and mitigates the risk of human error. However, the implementation of AI technologies in the anti-money-laundering and counter-terrorist-financing (AML/CFT) sector raises substantial legal questions, primarily concerning liability for decisions made by algorithms, the compatibility of such solutions with personal data protection standards, and the transparency of automated systems. In regulatory practice, striking an appropriate balance between operational efficiency and the protection of fundamental rights has become particularly important, necessitating an in-depth comparative analysis of existing legal frameworks and supervisory guidelines across various jurisdictions.

The literature on the application of AI in finance initially focused on the automation of routine tasks and the enhancement of basic compliance processes. However, with the advancement of sophisticated algorithms, greater data availability, and increased computing power, AI applications in AML/CFT have moved beyond operational automation—i.e., routine process execution, such as data ingestion and cleansing, entity resolution, and rule-based screening—towards analytical and decision-support functions, including machine-learning-based risk scoring, anomaly detection, and alert prioritisation (Ranković, *et al.*, 2023). In limited cases, they also support constrained automated decisions subject to documented human oversight. Contemporary scholarship identifies several theoretical perspectives on the use of AI in finance. The mechanistic approach, as used in this article, refers to the use of AI to automate routine compliance and business processes, such as data ingestion and cleansing, entity resolution, or the execution of rule-based scenarios, and emphasises AI's role in streamlining operational workflows (Arslanian and Fischer, 2019). By contrast, the analytical-predictive approach highlights the use of machine-learning models and data-analytic techniques for forecasting, classification, and decision support, for example in risk-scoring or anomaly-detection systems. AI is increasingly recognised as transformative in finance not because of its complexity per se but due to its demonstrated

and expected capabilities—including scalable pattern detection, near-real-time analysis, and adaptive decision-support.

Bibliometric analysis of existing publications reveals three dominant areas of research on AI in finance: (1) portfolio optimisation and decision-making models; (2) detection of financial fraud and credit risk assessment; and (3) sentiment analysis and market trend prediction (Goodell *et al.*, 2021). Notably, AI methods and subfields, in particular neural networks (including deep-learning variants) and natural language processing (NLP), are gaining prominence because they enable financial institutions to analyse complex, unstructured data (e.g., free-text narratives, documents, and media signals).

A significant aspect of the current academic discourse is the development of explainable AI (XAI), which aims to enhance the transparency of AI-based systems. These solutions respond to regulatory requirements and the growing expectations concerning the accountability of financial institutions for decisions made through automated processes (Yeo *et al.*, 2023, p. 189). Concurrently, a growing body of literature addresses regulatory challenges, focusing on the harmonisation of legal standards and regulatory risks arising from fragmented international approaches (Azzutti, 2024).

A growing body of regulatory research underscores a dual need: to bridge the gap between AI's capabilities and existing legal frameworks and to address AI-specific risks, including bias and unfair outcomes, opacity/non-explainability, and data-protection implications, within a risk-based approach. The literature underscores the importance of a comprehensive approach that integrates legal, ethical, and technological considerations (Fan *et al.*, 2025, p. 3; Mirishli, 2023, p. 40). FATF publications have been particularly active in this area, systematically exploring regulatory challenges and practical applications of AI in AML/CFT systems (FATF, 2021a, 2021b). The FATF emphasises AI's key role in automating customer risk analysis and detecting suspicious transactions while warning against the risks of infringing on fundamental rights, especially concerning data protection and the transparency of decision-making processes.

Compared with Germany and France, where the academic and supervisory literature on the use of AI/ML (artificial intelligence/machine learning) for anti-money-laundering is relatively mature, scholarship in Poland is still emerging. Although several studies have appeared in recent years, they largely address discrete topics—for example, the application of reinforcement learning (RL, a subfield of ML) in AML/CFT decision-making (Kędzierski, 2023) and the use of AI to counter economic cybercrime (Bukowski, 2023). However, a broader systemic approach and an in-depth analysis of the legal and ethical challenges arising from the implementation of AI by AML/CFT obliged entities – understood here as regulated financial institutions and designated non-financial businesses and professions (DNFBPs) that are subject to AML/CFT duties – are still lacking.

Similarly, in the Japanese academic context, the issue of AI application in AML/CFT is still in its nascent phase. Existing publications predominantly focus on the technical and practical aspects of AI deployment, while less attention is paid to the legal dimensions (Ozaki, 2019, pp. 342–343).

Despite the dynamic growth of international literature, there remains a clear research gap in the form of a lack of comprehensive comparative analyses that address both regulatory and practical aspects of AI implementation in AML/CFT systems. The objective of this article is to analyse and assess the regulatory and practical aspects of implementing AI-based solutions within AML/CFT systems in Japan while incorporating a comparative perspective drawn from Germany, France, and Poland. Specifically, the study identifies

regulatory gaps, contrasts supervisory approaches, and distils evidence-based recommendations for Japan. The detailed case-selection rationale (Japan; Germany, France, and Poland) is provided in the next section.

Research Framework and Methodology

The objective of this article is to analyse and assess the regulatory and practical aspects of implementing AI-based solutions within AML/CFT systems in Japan while incorporating a comparative regulatory perspective drawn from selected European Union member states (Germany, France, and Poland). In particular, the study identifies both intra-jurisdictional inconsistencies (gaps and tensions within each system, e.g., between AML duties and data-protection requirements) and cross-jurisdictional misalignments (divergences across Japan, Germany, France, and Poland relevant to transferability), and highlights legislative best practices that could be considered for adoption in the Japanese legal system.

Japan is treated as the focal case, while Germany, France, and Poland serve as purposively selected comparators based on supervisory/policy maturity, availability of authoritative sources, and shared GDPR–APPI/FATF baselines.

To achieve the research objective, the following specific questions are addressed:

1. What are the key legal challenges associated with the use of AI in Japan's AML/CFT system (e.g., liability for automated decision-making, data-protection compliance, and transparency/explainability)?

2. How do Germany, France, and Poland—selected as purposive comparators on the basis of supervisory maturity, source availability, and a shared GDPR baseline—converge with or diverge from Japan on these dimensions?

3. Which international standards and soft-law instruments are most relevant for governing the use of AI in AML/CFT systems, and how should they inform national frameworks (e.g., FATF Recommendations, the EU AML package and AI Act, OECD/IOSCO guidance)?

The research hypothesis assumes that the current legal frameworks in both Japan and the selected EU countries are inadequate with respect to the use of AI in AML/CFT systems. This inadequacy results not only in the risk of violations of fundamental rights but also in reduced effectiveness in combating money laundering and terrorist financing. Effective implementation in the Japanese context should be guided by the global baseline set by the FATF Recommendations and informed by EU standards—namely the GDPR, the AI Act, and the 2024 EU AML package—used here as comparative benchmarks for Japan to strengthen data protection, accountability for automated decisions, and the transparency/explainability of analytical systems.

Methodologically, the study employs doctrinal legal analysis and normative comparative methodology, supplemented, where appropriate, by elements of functional comparison. The doctrinal approach enables a detailed examination of applicable legal norms, judicial decisions, and administrative documents, allowing for precise identification of their scope, legal loopholes, and contentious issues. The comparative method facilitates the juxtaposition of different legal systems and regulatory practices to identify optimal legislative solutions suitable for implementation, while the functional perspective is used

in a limited, illustrative manner to assess the operational feasibility of selected mechanisms, such as data protection impact assessments (DPIAs), explainability documentation, and human-in-the-loop controls—based on statutory/supervisory sources and reported practices, rather than a full empirical evaluation.

The substantive scope of the study covers the use of AI in the field of anti-money laundering and counter-terrorist financing. Geographically, the analysis is centred on Japan and selected EU countries (Germany, France, and Poland). The temporal scope covers May 2015–May 2025, capturing the main reform wave in AML/CFT and AI governance. This interval spans the EU's post-2015 AML reform cycle (AMLD IV and subsequent measures), the adoption and application of the GDPR (2016/2018), Germany's recast GwG (2017), Japan's APPI amendments (2020/2022) and JFSA guidance (2021/2023), the FATF (2021a, 2021b) reports on new technologies, the 2024 EU AML package and AI Act, and early 2025 supervisory materials (e.g., the JFSA AI discussion paper).

This article adopts a purposive comparative design focusing on Japan and three EU jurisdictions – Germany, France, and Poland. The selection rests on three considerations. First, Japan couples high technological capacity with a privacy-centric regulatory posture (APPI, JFSA guidance), making it a salient case for assessing a legally robust deployment of AI in AML/CFT. Second, Germany and France exhibit mature and well-documented supervisory guidance and practice (e.g., BaFin principles; AMF/Tracfin materials), which provide concrete benchmarks on explainability, auditability, and human-in-the-loop controls. Third, Poland represents an emerging scholarly and supervisory context within the EU AML package and the GDPR. Taken together, this purposive selection spans a spectrum of regulatory maturity within broadly similar civil-law traditions and supports the derivation of transferable, evidence-based recommendations for Japan. The comparison is instrumental rather than exhaustive.

AI is understood here as machine-based systems that, with varying levels of autonomy, infer from input data how to generate outputs (predictions, classifications, recommendations, alerts) for AML/CFT tasks, such as data analysis, risk assessment, and the detection of suspicious activities. In this article, an algorithm denotes a finite, explicit, and unambiguous procedure for transforming inputs into outputs. Such algorithmic techniques are treated as AI only when they implement inferential, model-based approaches (e.g. ML or NLP models) or exhibit adaptiveness beyond fixed rules, echoing the functional distinction drawn in international guidance on new technologies for AML/CFT (FATF, 2021b). Purely deterministic, rule-based engines are classified as automation rather than AI. This working definition is functionally scoped to AML/CFT compliance and provides analytical clarity; it complements rather than replaces statutory or supervisory definitions.

This is a legal–comparative study. While it draws on technical and policy sources for context, it does not provide an engineering-level examination of AI models or an empirical audit of deployments. Technical elements are included only insofar as they illuminate legal implications. Furthermore, due to the rapid pace of technological development and evolving regulatory frameworks, subsequent updates to the legal landscape may not be fully reflected in this article. Economic and socio-political dimensions are mentioned only briefly, without in-depth empirical analysis; this aspect may constitute a promising avenue for future research. An additional limitation is the potential bias resulting from the uneven availability of sources in English, which may have influenced the level of detail in the analysis of individual jurisdictions.

Additionally, it should be noted that some of the observed differences between jurisdictions may stem not only from divergences in the substantive legal provisions but also from

variations in regulatory cultures, institutional traditions, and enforcement practices. For example, jurisdictions with a more proactive compliance ethos or stronger institutional capacities may achieve higher levels of AI integration in AML/CFT systems even under broadly similar legal frameworks. This cultural and institutional dimension, while outside the primary normative focus of this study, inevitably influences the comparative findings and should be considered when interpreting the results.

Discussion – The Use of Artificial Intelligence in AML/CFT Systems: A Comparative Analysis of Japan, Germany, France, and Poland

Normative and definitional foundations

In the AML/CFT context, AI is gaining increasing relevance as a tool for automating risk analysis, client profiling, and the detection of unusual transactions. Nevertheless, the concept of 'artificial intelligence' is not uniformly defined in either international or national legal documents, which may hinder its regulation and implementation in accordance with the principles of legality, proportionality, and transparency.

In documents prepared by the FATF, AI is presented as a component of a broader ecosystem of advanced technologies supporting digital transformation in the financial sector. In its report titled *Opportunities and Challenges of New Technologies for AML/CFT* (FATF, 2021b), FATF does not offer a closed, universal definition of AI but rather characterises it based on its capacity to analyse large datasets, identify patterns, and support real-time decision-making. The organisation emphasises that AI methods and subfields—in particular machine learning (ML) and natural language processing (NLP)—can significantly enhance AML/CFT effectiveness. Simultaneously, the FATF stresses the need for regulatory and supervisory frameworks that enable institutions to manage AI-specific risks, such as bias and unfair outcomes, opacity/non-explainability, privacy and data-protection issues, and automation without meaningful human oversight (including risks of 'digital de-risking'/exclusion).

At the level of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council, commonly known as the Artificial Intelligence Act (AI Act), contains one of the most precise definitions of AI within the European legal space. AI is defined as follows:

> AI system' means 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 (European Commission, 2021, Article Art. 3(1)).

This regulation encompasses a broad spectrum of systems, including both rule-based algorithms and machine learning models.

In Japan, although there is no single statute that defines AI, the JFSA (2025) employs the term "AI systems" in its regulatory guidelines in reference to analytical tools that support risk assessment, decision-making, and transaction monitoring. In its materials, the JFSA treats AI functionally rather than via a single statutory definition. The 2025 AI Discussion Paper, without prescribing a technical definition, distinguishes between 'conventional AI' and 'generative AI', and identifies concrete use cases in risk controls (including AML/CFT),

e.g., transaction-monitoring models trained on historical data, sometimes combined with rules-based systems or developed jointly across financial institutions; by comparison, the 2021 AML/CFT Guidelines set expectations for IT systems, data governance, and risk-based controls but do not define AI as such.

As EU member states, Germany and France are bound by the EU AI Act's definition of an "AI system" (Regulation (EU) 2024/1689, Article 3(1)). In Germany, BaFin's (2021) principles on the use of algorithms emphasise transparency, validation, and supervisory oversight; they operate alongside—rather than in place of—the AI Act definition and its forthcoming obligations for high-risk systems.

In France, the AMF has not issued a standalone statutory definition specific to financial services. In practice, French supervisors apply the AI Act definition together with GDPR-based obligations on profiling, transparency, and DPIAs. In particular, the AMF contributed to the IOSCO (2024) report entitled "Artificial intelligence in capital markets: use cases, risks, and challenges." This report examines the applications, risks, and challenges of AI in capital markets. The French regulator defines AI as an 'automated decision-making process based on statistical models and algorithms' and highlights the risks related to non-explainability and potential algorithmic discrimination.

In Polish documents issued by the General Inspector of Financial Information (GIIF) and the Polish Financial Supervision Authority (KNF), the term 'artificial intelligence' is mainly discussed in the context of future supervisory challenges. These documents do not provide a precise definition of AI, but rather references are made to broadly understood systems that automate AML risk assessment or assist in identifying suspicious transactions.

Despite the absence of a unified definition, practice and academic literature allow for the identification of core functions performed by AI systems in the AML/CFT context:

- **Classification** – AI analyses input data to categorise entities, transactions, or behaviours according to risk levels (e.g. low-/high-risk clients).
- **Prediction** – systems trained on historical data predict the likelihood of undesirable events, such as attempted money laundering.
- **Profiling** – analysis of client behaviour to develop patterns (e.g. payment schemes) that can be used to detect deviations and anomalies.
- **Alerting and anomaly detection** – AI generates automated alerts when it detects behaviour that deviates from 'normal' patterns, thus supporting the operation of monitoring systems.

Each of these functions involves distinct legal challenges—ranging from the transparency of decision-making models, the legality of profiling to accountability for false positives or false negatives.

The use of AI in AML/CFT systems has been recognised and addressed in the documents of key international organisations, such as the FATF (IOSCO, 2024) and OECD (IOSCO, 2024). As international standard-setters without direct law-making authority, these organisations do not provide binding regulations for AI implementation; rather, they issue non-binding principles and guidelines that inform and steer the design and deployment of modern technologies, including AI, in the financial sector. In its 2021 report titled *Opportunities and Challenges of New Technologies for AML/CFT*, the FATF

recognised the considerable potential of AI and related technologies, such as big data, machine learning, and automated pattern recognition, in enhancing compliance processes under AML/CFT regimes. According to the FATF, these tools can significantly improve the effectiveness of anti-money laundering measures by enabling faster and more accurate identification of suspicious transactions, enhanced customer profiling, reduced false positives, and more efficient allocation of compliance resources (IOSCO, 2024). At the same time, the FATF explicitly warns against the risks associated with opaque or inadequately supervised deployment of AI solutions (IOSCO, 2024, pp. 42–43). In particular, the report emphasises the need to ensure that new technologies remain transparent and accountable; regarding transparency, financial institutions must understand how AI systems operate, and regulators must be able to exercise effective oversight; regarding accountability, despite automation, ultimate responsibility for decisions must rest with a human or the institution. Aligned with the risk-based approach, AI implementation should be problem- and risk-driven, with a demonstrated need and proportionality, rather than technology-first adoption. The FATF warns about the risk of 'digital de-risking'. Client exclusion occurs when high-sensitivity scoring raises false positives and triggers threshold-based denials (onboarding/off-boarding) without individualised review. This 'digital de-risking' risks breaching proportionality and equal-treatment standards, especially with opaque models, biased data, or weak human oversight. This framing is consistent with international standards and supervisory expectations on risk-based AML/CFT, automated decision-making, and AI governance, including FATF guidance on the risk-based approach and (digital) de-risking (FATF, 2021a, 2021b), the GDPR provisions on automated decisions, and data minimisation (Arts 5(1)(c) and 22; European Parliament and Council, 2016), BaFin's (2021) principles on the use of algorithms in decision-making as well as recent securities and financial-sector guidance on AI risks and supervisory expectations (IOSCO, 2024; OECD, 2024).

Although not an AML authority per se, the OECD has published a range of analyses on the application of AI and digital technologies in the financial sector, including in the context of supervision and regulatory compliance. In its 2024 report titled *Regulatory Approaches to Artificial Intelligence in Finance*, the OECD (2024, pp. 17, 42) underscored the importance of AI and RegTech as tools that can enhance supervisory efficiency, risk identification, and regulatory compliance. At the same time, the OECD identified key barriers to AI adoption, such as lack of system interoperability, limited institutional resources, and legal uncertainty surrounding existing regulatory frameworks. Among its recommendations, the report advocates the development of national digital strategies for financial supervision and the expansion of regulatory sandboxes, which allow for testing of innovative—AI-based—solutions under controlled conditions and with the involvement of supervisory authorities.

The application of AI in AML/CFT systems is grounded in existing legal frameworks, typically indirectly via risk-based obligations on institutions to identify, assess, and monitor risks (e.g., customer due diligence and ongoing monitoring duties). Normatively, the analysis is anchored in global and domestic AML/CFT standards. At the international level, it draws on FATF (2021) recommendations 1 (risk-based approach), 10 (customer due diligence), and 15 (new technologies). In the EU context, it relies on the new EU AML regulation (Regulation (EU) 2024/1624), the associated directive (Directive (EU) 2024/1640), and the GDPR, where profiling and automation are involved (Regulation (EU) 2016/679). For Japan, the key reference points are the Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007, e.g. Arts 6 and 8; Government of Japan, 2007) and the JFSA AML/CFT guidelines (2021/2023). The German and Polish examples are framed, respectively, by the Money Laundering Act (Geldwäschegesetz – GwG, 2017) and the Polish AML Act of 1 March 2018 (Arts 33–34 on ongoing relationship

monitoring and unusual transactions). In the jurisdictions analysed, Japan, Germany, France, and Poland, there is no comprehensive legislation specifically regulating the use of AI in AML/CFT. Nevertheless, each of these jurisdictions features general provisions that indirectly shape the legal framework for the implementation of AI tools in the financial sector, along with guidance issued by supervisory authorities that indicate preferred practices in this domain.

In Japan, the primary piece of legislation regulating anti-money laundering is the Act on Prevention of Transfer of Criminal Proceeds, enacted in 2007 (Act No. 22 of 2007; Government of Japan, 2007). While the act does not directly address technological issues, Articles 6 and 8 impose on obliged institutions the duty to apply 'appropriate and effective measures' in client identification, transaction monitoring, and the reporting of suspicious activity. This language is interpreted as permitting the use of advanced technologies, including machine learning and predictive algorithms. A second key piece of legislation is the APPI (Act No. 57 of 2003), as amended in 2020/2022, which, through its 2020 and 2022 amendments, introduced important provisions concerning automated data processing, including the obligation to inform individuals subjected to profiling and the requirement to conduct privacy impact assessments. This implies that the use of AI in AML—particularly in client scoring—must comply with the principles of transparency and proportionality. The legal framework is complemented by the AML/CFT guidelines of the JFSA (Financial Services Agency, 2023b), especially those issued in 2021 and 2023, which formalise expectations for financial institutions concerning the use of digital tools, including the need to maintain human oversight over algorithms and to document the decision-making logic.

In Germany, the key legislative act is the *Geldwäschegesetz* (Government of Germany, 2017), updated in line with successive EU AML directives. Although the act does not explicitly regulate AI, Articles 25 to 27 impose an obligation to maintain an effective risk management system and to conduct independent audits of tools used in AML procedures. Accordingly, AI-based tools—when applied—are subject to the same obligations as traditional IT systems, or even stricter requirements given their autonomous nature. AI implementation in Germany must also comply with the GDPR (European Parliament and Council, 2016). The German approach provides for strict data protection, and automated individual decision-making—such as flagging a transaction as suspicious without human involvement—is permissible only under the conditions of Article 22 of the GDPR. In practice, this necessitates the ability to verify decisions and to inform the customer about the logic behind the algorithm. The Federal Financial Supervisory Authority (BaFin) plays a significant role through publications such as Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen (BaFin, 2021), which set standards for algorithm transparency, validation, and supervision. BaFin emphasises that any use of AI must allow for retrospective analysis and error control. Read together, the GwG, the GDPR, and BaFin's 2021 principles impose concrete design constraints. Systems must be auditable and traceable (documented model inventories, reproducible alert trails, controlled change-management), sufficiently explainable to permit notice and challenge without tipping-off, and subject to meaningful human involvement for adverse decisions. They also require ex-ante validation and ongoing monitoring (back-testing, drift surveillance, false-positive calibration) as well as data-protection-by-design (DPIA, minimisation, purpose limitation, and vendor oversight). The practical consequence is that high-opacity architectures are disfavoured, and AI deployment is viable only under robust governance and documentation.

In France, the regulatory foundation is provided by the Code Monétaire et Financier (Légifrance, 2025), which defines the AML/CFT obligations of financial institutions,

including the principle of proportionality between technological measures and risk levels. In practice, this implies that banks and other entities may -and indeed should -apply advanced technologies, such as AI, in cases where traditional mechanisms are inadequate. This framework is supplemented by the *Loi Informatique et Libertés* (French Data Protection Act; Centraleyes, n.d.), which transposes the GDPR into French law and lays out specific conditions for profiling and automated decision-making concerning natural persons. According to interpretations by the Commission Nationale de l'Informatique et des Libertés (CNIL), AML scoring based on AI requires DPIAs and assurances of system transparency. Furthermore, the AMF (2022) and the financial intelligence unit Tracfin (2023) have issued a series of recommendations on the use of machine learning algorithms, stressing the need for explainability and limiting their use in decisions with serious consequences for clients. France also stands out for its high level of institutional integration between regulators and obliged entities, exemplified by joint regulatory initiatives and sectoral consultations concerning algorithmic accountability.

In Poland, the primary source of substantive law in the area of AML/CFT is the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (Poland, 2018). Articles 33–34 of the Act impose an obligation on obliged institutions to continuously monitor business relationships and to identify unusual transactions. Although the Act does not explicitly refer to AI technologies, a functional interpretation permits their use as a supporting tool for transaction analysis, provided they do not violate the principles of adequacy and proportionality. At the same time, the application of AI must comply with the provisions of GDPR, which prohibits fully automated decision-making that produces significant legal effects, unless the data subject has given explicit consent or the decision is necessary for the performance of legal obligations.

Unfortunately, the General Inspector of Financial Information (GIIF), acting within its statutory competences, has not issued any public guidance for obliged institutions regarding the use of AI, machine learning, or other advanced systems and solutions in AML/CFT practice (Generalny Inspektor Informacji Finansowej [GIIF], n.d.). In contrast, the Polish Financial Supervision Authority, KNF, through its "FinTech Sandbox" initiative, actively promotes the development of technological innovations - including AI - while underscoring the need to ensure adequate legal, organisational, and technical safeguards (KNF, 2019).

Against the backdrop of domestic regulations, the future of AI in AML/CFT systems will be shaped not only by the EU AML legislative package - namely Directive (EU) 2024/1640 (AMLD VI, Directive (EU) 2024/1640; European Parliament and Council, 2024a), Regulation 2024/1624 (Regulation (EU) 2024/1624; European Parliament and Council, 2024c), and Regulation (EU) 2024/1620 establishing the European Anti-Money Laundering Authority (AMLA, Regulation (EU) 2024/1620; European Parliament and Council, 2024b) – but also by the horizontal Artificial Intelligence Act, Regulation (EU) 2024/1689 (Regulation (EU) 2024/1689; European Parliament and Council, 2024d). The AI Act introduces a harmonised definition of an AI system and cross-sectoral obligations (e.g., risk management, data governance, technical documentation/logging, transparency to users, human oversight, and accuracy/robustness/cybersecurity) that will apply in parallel to AML/GDPR requirements where relevant. Announced in 2021 and progressively refined in subsequent years, this package represents a qualitative shift in the EU's approach to countering money laundering and terrorist financing. Of particular relevance to AI are the provisions of a draft AML Regulation, which—unlike previous directives—will be directly applicable in all member states. This regulation addresses the automation of analytical processes for the first time, emphasising the need to ensure compliance with the principles of transparency, auditability, and respect for individual rights (Regulation (EU) 2024/1624, Article 76(5)).

One of the key challenges for obliged institutions will, thus, be the integrated application of several legal regimes simultaneously: the proposed AML Regulation, the AI Act, and the GDPR. For a more detailed, sector-specific discussion focused on banking supervision and AI-driven oversight, see Azzutti *et al.* (2024). In practice, this will require designing systems that are compliant with the principle of privacy by design while also capable of demonstrating effectiveness in combating money laundering. Although the EU AML package does not regulate AI in an exhaustive manner, its provisions lay the groundwork for a more coherent and harmonised approach to the implementation of digital technologies in the financial sector.

In this context, it must be emphasised that a lack of coordination between AML, data-protection, and AI-oversight regimes may produce normative conflicts, over-regulation, or even decision-making paralysis. An additional, unintended consequence is that contrasting or poorly sequenced requirements can jeopardise effective and safe AI deployment by increasing regulatory uncertainty and inhibiting investment in compliant system design. Therefore, future legislative efforts should aim at harmonising and aligning the respective requirements so as to ensure, on the one hand, the effectiveness of the AML/CFT system and, on the other, the full protection of fundamental rights and legal certainty regarding the permissible scope of AI use. In the long term, European AML supervision—combined with the evolving AI regulatory ecosystem—may offer a model for the effective, responsible, and legally compliant use of technology in the service of financial security.

Critical Assessment and Comparative Analysis

The analysis proceeds on two levels, namely intra-jurisdictional (within each legal system) and cross-jurisdictional (across the four jurisdictions), to isolate system-specific gaps and comparative misalignments. Against common benchmarks—FATF's risk-based approach, the GDPR (incl. Art. 22 safeguards), and the EU AI Act's high-risk requirements—the four jurisdictions show asymmetric capacity to operationalise AI in AML. Germany and France display higher supervisory maturity (codified expectations on explainability, auditability, and human oversight); Japan relies on general APPI duties and soft-law guidance with limited AML-specific AI rules; Poland is EU-aligned but remains sector-thin on AI guidance. Cross-cutting weaknesses persist: liability for algorithmic outcomes is under-specified; transparency and explainability requirements frequently collide with anti-tipping-off constraints; and DPIA/data-minimisation duties can constrain data-hungry models unless proportionately justified.

The most fundamental issue is the absence of precise legal provisions concerning liability for decisions made by AI in AML/CFT systems. None of the jurisdictions examined has thus far introduced clear legislative solutions indicating who bears responsibility—and to what extent—for erroneous, ineffective, and discriminatory outcomes generated by algorithms. In practice, this area remains governed by the general principles of civil, administrative, or criminal liability applicable to obliged institutions or their employees, without taking into account the specific nature of machine learning systems. The lack of explicit norms raises significant interpretive uncertainty, particularly in the context of deep learning tools, whose decisions may be difficult to explain and subject to post-hoc review. Some illustrative liability scenarios are given below:

(i) False negative/missed STR. An obliged institution deploys an ML-based alert-prioritisation model. Due to thresholding or model drift, a high-risk pattern is down-scored and no suspicious transaction report (STR) is filed. Following a law-enforcement investigation, the supervisor sanctions the institution for failures of ongoing monitoring

and STR obligations; internal accountability may extend to senior management under governance rules. Contractual recourse may be sought against a vendor (e.g., breach of validation/quality warranties), but primary liability remains with the obliged institution.

(ii) False positive/'digital de-risking'. An automated high-risk score triggers account closure or onboarding denial without meaningful human review or an intelligible explanation. The customer challenges the decision under data-protection rights (GDPR, Articles 5, 15, and 22) and equal-treatment norms; damages or corrective orders may follow where proportionality or lawful basis is not demonstrated. Certain dynamics shape design choices (auditability, explainability, human-in-the-loop, calibration and drift monitoring) yet remain legally uncertain due to the absence of AI-specific liability standards.

Another major challenge lies in striking an appropriate balance between the effectiveness of AI systems and the requirements of transparency and privacy protection, especially in the light of data protection regulations. AI-based AML systems often process vast datasets—including sensitive data—and conduct client profiling in ways that are difficult to predict or control (Kuiper *et al.*, 2021, p. 2). Germany and France have developed relatively advanced standards concerning algorithmic transparency and customer information obligations. However, even in these jurisdictions, the contours of transparency and customer-information duties are actively debated in case law and guidance. The Court of Justice of the European Union's (CJEU) SCHUFA (Schufa Holding AG) ruling, for instance, expands the reach of GDPR Article 22 to certain credit-scoring practices and stresses the provision of "meaningful information about the logic involved" (CJEU, 2023; European Parliament and Council, 2016, Article 22). In parallel, guidelines on automated decision-making and profiling issued by the former Article 29 Working Party, 2018, and endorsed by the European Data Protection Board (EDPB), clarify transparency, information, and contestation duties for automated decisions (Article 29 Working Party, 2018). French and German supervisory materials likewise set explainability and documentation expectations—both CNIL's (2025) recent AI recommendations and BaFin's (2021) principles foreground explainability, documentation, and oversight—yet leave open tensions with trade-secrets constraints and tipping-off prohibitions in AML/CFT contexts. Poland shares the GDPR baseline with Germany and France. The divergence lies not in statutory text but in sector-specific supervisory guidance. While BaFin and French authorities, such as CNIL and Tracfin, have articulated expectations on explainability, DPIAs, and automated decision-making in financial services (BaFin, 2021; CNIL, 2025; Tracfin, 2023), Poland's GIIF and KNF have not issued AML/AI-specific guidance beyond general GDPR duties (GIIF, n.d.; KNF, 2019). Japan similarly applies the Act on the Protection of Personal Information together with JFSA materials that impose general transparency and privacy impact assessment (PIA)-type obligations but do not set financial sector-specific rules for AI-driven profiling (Financial Services Agency, 2023a; Government of Japan, 2003; JFSA, 2025). As a result, obliged institutions are often forced to interpret the permissible scope of their activities on their own, which leads to discrepancies in practice and increases the risk of infringing upon clients' fundamental rights.

Regulatory imprecision also extends to the principle of human-in-the-loop, which requires that final decisions in AML systems—especially those with significant legal or financial consequences—be made with human involvement. Supervisory bodies such as BaFin, the JFSA, and the GIIF refer to this principle in their guidance. However, it is not clearly stated in the law and lacks detailed implementation rules. The AI Act partially addresses this gap: for high-risk AI systems, Title III requires effective human oversight. Providers must design oversight measures and instructions enabling natural persons to detect anomalies, intervene, and override/stop the system; deployers must ensure competent, empowered reviewers with training on system limits. In AML settings, AI applications

that support or influence decisions that significantly affect individuals' access to financial services may fall within the high-risk perimeter; in that case, the AI-Act oversight duties apply alongside GDPR Art. 22 safeguards (right to obtain human intervention) and AML secrecy/tipping-off constraints. Yet sector-specific parameters – what counts as meaningful review, evidentiary thresholds, timelines, and documentation standards-remain under-specified in positive law, even though framework-level requirements on high-risk AI and automated decision-making exist in the AI Act and the GDPR and are elaborated in supervisory guidance (Regulation (EU) 2024/1689, Title III; European Parliament and Council, 2016, Article 22; Article 29, Working Party, 2018; BaFin, 2021). As a result, in practice, human oversight is often ineffective. In some cases, AI systems operate in a fully automated mode, with human involvement reduced to passive approval of alerts—an approach that runs counter to the spirit of data protection and proportionality regulations. A further complication is the absence of clear criteria to assess whether human oversight was genuine or merely formal. In EU data-protection terms, 'meaningful' human oversight requires an active, informed review by a person with authority to alter the outcome. Mere rubber-stamping of automated alerts is insufficient, as reflected in data protection and supervisory guidance on automated decision-making and human review (Article 29, Working Party, 2018; BaFin, 2021; FATF, 2021; Information Commissioner's Office (ICO), 2020).

The above-mentioned gaps and inconsistencies point to the urgent need for in-depth legislative reflection and the harmonisation of national laws with international standards—particularly with the FATF recommendations and the requirements of GDPR. Without such alignment, the deployment of AI in the AML/CFT sector will face increasing legal and ethical risks, and its effectiveness may be seriously undermined by a lack of public trust and regulatory uncertainty.

The use of AI in AML/CFT systems entails significant risks to personal data protection, especially in relation to profiling, automated decision-making, and processing transparency. In the countries analysed—Japan, Germany, France, and Poland—this issue is regulated to varying degrees. However, a common denominator is the shared need to reconcile the requirements of effective financial crime prevention with the protection of individual rights.

One of the key issues concerns the legality of profiling and automated decision-making under data protection regulations. Under the GDPR (Article 22), individuals are not subject to decisions that produce legal effects concerning them or significantly affect them if such decisions are based solely on automated data processing, including profiling, unless certain exceptions apply. These exceptions include situations where the decision is necessary for the performance of a contract, authorised by Union or member state law, or based on the explicit consent of the data subject. In the context of AML/CFT, particular attention is given to the legal basis arising from the statutory obligations imposed on obliged institutions, for example, under national AML laws. However, in all cases, the implementation of so-called appropriate safeguards is required, including the right to human intervention, the opportunity to express one's point of view, and the ability to contest the decision.

In Germany, which traditionally adopts a strict approach to data protection (DSGVO), there is a strong emphasis on limiting the use of full automation in AML-related decisions. The deployment of AI tools must be designed so that decisions such as denying a business relationship or submitting a suspicious transaction report (STR) to the financial intelligence unit are not made solely by algorithms without human involvement. In France, according to the interpretation of CNIL and the Loi Informatique et Libertés,

profiling in the financial sector—even when intended to counter criminal activity—must meet high standards of transparency and must demonstrate purposefulness and proportionality of the measures applied.

As an EU member state, Poland applies the GDPR baseline: solely automated decisions producing legal or similarly significant effects are restricted unless an exception applies and safeguards are ensured. In AML contexts, onboarding/off-boarding and STR-related escalations, therefore, require meaningful human review and intelligible information about the logic involved, subject to tipping-off limits. Sector-specific supervisory guidance remains limited: the GIIF has not issued AI/AML-specific public guidance, and KNF materials (e.g., sandbox) are technology-general rather than AML-specific.

Under APPI and JFSA AML/CFT guidance, obliged entities must ensure transparency, appropriate/effective monitoring measures, and documented oversight of analytical tools. The JFSA frames governance and human oversight for AI use cases (including AML/CFT), while APPI requires purpose transparency and privacy-impact assessments for higher-risk processing. However, there is no express statutory analogue of GDPR Art. 22. Consequently, human-in-the-loop and explainability expectations arise chiefly from soft-law and general APPI principles, placing a premium on documented human review, explainability, and appeal channels where AI supports adverse outcomes.

Closely related to this is the transparency requirement and the right to obtain an explanation, which also derives from the GDPR (Articles 5, 15, and 22). Individuals whose data are processed within AML/CFT procedures using AI have the right to understand the logic of the system's functioning and how decisions are made. In practice, this necessitates the application of the principle of AI model explainability—particularly difficult to achieve in the case of complex deep learning algorithms. The regulatory challenge lies not only in providing the client with an intelligible account of the decision-making mechanisms but also in enabling effective oversight of such systems by regulatory authorities. Recent CJEU case law tightens explainability for automated decision making (ADM). In the *SCHUFA* case (Case C-634/21, 7 December 2023), the Court held that credit scoring itself can constitute ADM under Art. 22 of the GDPR where third parties rely on it decisively for contractual outcomes (CJEU, 2023). In *CK v Dun & Bradstreet* (Case C-203/22, 27 February 2025), the Court clarified that Art. 15(1)(h) of the GDPR requires meaningful information about the logic involved - including key parameters and their influence – without mandating the disclosure of the full algorithms. Trade-secret claims cannot justify an absolute refusal; a case-by-case balancing is required and may involve disclosure to the supervisory authority or court (CJEU, 2025).

Documents issued by BaFin—and, in Poland, general KNF governance materials—stress the need to document decision-making processes and to ensure they are auditable, internally and externally.

Another important legal requirement is the obligation to conduct a data protection impact assessment (DPIA), pursuant to the (Article 33). Such an assessment is mandatory when data processing is likely to result in a high risk to the rights and freedoms of natural persons, especially where systematic monitoring, automation, and new technologies are involved. The use of AI in AML/CFT, by definition, meets these criteria, which means that every obliged institution implementing AI must assess potential privacy risks prior to deployment, evaluate the proportionality and necessity of the processing, and design adequate risk-mitigation measures. Failure to carry out a DPIA constitutes a breach of data protection rules and may result in administrative sanctions.

Of particular significance is the principle of data minimisation (Article 5(1)(c) of the GDPR, as well as analogous provisions in Japan's APPI and the French data protection law), which requires that data be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. In the context of AI, this may mean limiting the scope of data fed into learning systems and verifying that the processing does not include information unnecessary from the perspective of AML obligations. For a sector-specific discussion in banking supervision that links proportionality, data governance and AI deployment, see Azzutti (2024). In practice, failure to observe this principle can lead to excessive invasions of privacy and increase the risk of systemic errors and discriminatory outcomes.

A cross-jurisdictional legal assessment of the frameworks and supervisory materials governing the use of AI in AML/CFT in Japan, Germany, France, and Poland reveals significant differences, which stem not only from the technological advancement of each country but also from the nature of their legal systems, institutional maturity, and regulatory cultures. Despite sharing a common goal - improving the detection and analysis of financial risks - their approaches diverge, making full harmonisation and the maintenance of a uniform international compliance standard difficult.

Japan has strong technological and innovation capacity, with advanced work in robotics, machine learning, and big data, as reflected in recent supervisory materials and international assessments (Financial Services Agency, 2023a; JFSA, 2025; OECD, 2024). Nevertheless, AI adoption in AML/CFT has proceeded cautiously, reflecting a conservative regulatory posture and a privacy-centric APPI framework, complemented by JFSA soft-law guidance and academic analysis of Japan's approach to new technologies in AML/CFT (Financial Services Agency, 2023a; Government of Japan, 2003; JFSA, 2025; Ozaki, 2019). The Japanese legal system is characterised by an emphasis on legislative stability and conservatism, and there is a lack of detailed legal regulations directly addressing AI deployment in the fight against financial crime. While JFSA guidelines refer to new technologies, they are general and non-binding. Furthermore, restrictions under the APPI—particularly regarding profiling and individual consent—require that AI implementations be carefully designed, which slows down the deployment process. As a result, Japan presents itself as a country with advanced digital infrastructure but a cautious approach to the use of AI in regulated areas—especially AML/CFT, which touches on sensitive aspects of sovereignty and national security.

By contrast, Germany and France have adopted more systemic approaches to integrating AI tools into their domestic AML/CFT regimes while maintaining high standards of personal data protection in line with the GDPR. In both countries, AI is implemented as part of a comprehensive risk management model that includes auditability, transparency, and accountability of obliged entities. BaFin and the AMF, as financial regulators, actively participate in consultations on predictive technologies and regularly publish guidelines and best practices on machine learning, profiling, and process automation in AML. Importantly, these regulators promote XAI standards and provide obliged institutions with tools for assessing technology compliance with data protection regulations, such as checklists and risk assessment matrices. Germany and France thus exhibit greater institutional maturity in terms of both AI use in AML/CFT and in ensuring these systems comply with ethical and legal standards, as reflected in BaFin's (2021) principles on algorithm governance and validation, CNIL's (2025) recommendations on explainability, DPIAs and human oversight, and AMF (2022)/Tracfin (2023) contributions to international standard-setting, including through IOSCO (2024) work on AI in capital markets.

http://doi.org/10.35467/sdq/214090

Poland, compared to the above countries, is still in the process of building the legal and institutional infrastructure necessary for broader AI implementation in the AML/CFT sector. Although obliged entities—particularly the largest banks—are testing automated solutions for risk classification and anomaly detection, uniform standards and clear supervisory guidance remain lacking. The General Inspector of Financial Information (GIIF) has not yet issued a comprehensive document addressing the use of AI in AML, and the Polish Financial Supervision Authority (KNF) promotes only general innovation principles through a regulatory sandbox. AI adoption in Poland, therefore, takes place in a context of regulatory uncertainty and is largely driven by private sector initiatives. At the same time, GDPR obligations impose high requirements which - given the absence of sector-specific guidelines - may be interpreted inconsistently, resulting in compliance instability and limited trust in decision-making algorithms.

In conclusion, the differences in the maturity of AI integration into AML/CFT systems reflect not only the technological capabilities of individual countries but also, and more importantly, their respective approaches to balancing innovation with individual rights. Japan remains a technological leader with a cautious legal stance; Germany and France implement AI within harmonised regulatory frameworks; while Poland is still laying the foundations for coherent development in this domain. In the long term, it will be essential for these countries - regardless of their current stage - to strive for greater regulatory harmonisation and the exchange of best practices, in line with the international standards set by the FATF and the EU's digital strategy.

Conclusions, Recommendations, and Prospects for Future Research

The regulatory and comparative analysis of the implementation of AI in AML/CFT systems in Japan, Germany, France, and Poland has made it possible to identify key challenges and best practices concerning compliance with data protection regulations, accountability for automated decisions, and algorithmic transparency. The study found that although all analysed countries permit the use of AI in the AML/CFT sector, their approaches vary significantly in terms of regulatory scope and institutional maturity.

In response to the first research question, it was found that Japan, despite its high technological potential, operates under relatively general legal frameworks that lack specific provisions regarding liability for decisions made by AI. The Act on the Protection of Personal Information (APPI) imposes general obligations concerning transparency and data protection impact assessments (DPIAs), but it fails to address the specific characteristics of machine learning. The JFSA guidelines refer to AI, but these take the form of soft law and do not impose concrete obligations.

The second research question led to the conclusion that Germany and France have achieved a higher level of harmonisation between AML regulations and data protection requirements stemming from the GDPR. Both countries implement the principles of explainability, auditability, and human-in-the-loop oversight. Poland remains in the process of developing a systemic approach to AI in AML, with some regulatory awareness and initiatives, such as regulatory sandboxes, emerging. However, sector-specific guidelines from Poland's financial intelligence unit (GIIF) are lacking, and the Polish Financial Supervision Authority (KNF) has yet to establish a coordinated approach to AI in AML/CFT.

In the context of the third research question, the analysis showed that FATF standards play a key role in shaping approaches to AI in AML/CFT. First, Recommendation 1 (risk-based

approach) anchors proportionality, governance, and calibration for AI-supported monitoring. Second, Recommendation 15 (new technologies) and its interpretive materials require institutions to identify, assess, and mitigate technology-related risks. Third, FATF's 2021 reports translate these expectations into operational guidance on data governance, validation, explainability, and oversight, while warning against "digital de-risking"and clarifying how Recommendations 1 and 15 apply to new technologies (FATF, 2021a, 2021b, 2025). Although these standards are formulated as general guidelines, they explicitly call for AI systems to comply with the principles of transparency, accountability, and data protection. Nevertheless, their national implementation remains fragmented and uncoordinated.

The research hypothesis—which assumed that the current state of legal regulation of AI in AML/CFT systems in Japan and selected EU countries is insufficient—was confirmed. The analysis demonstrated that none of the examined jurisdictions has adopted coherent, comprehensive legal frameworks that adequately reflect the specific characteristics of AI technologies, particularly in the contexts of algorithmic profiling, decision-making, and the processing of large data sets. Guidelines and laws exist, but they are too general and imprecise. AML, data protection, and AI regulations are poorly coordinated. This creates legal gaps and increases the risk of non-compliance.

In the light of the above, it is recommended that Japan undertake legislative measures to clarify the rules on accountability for decisions made by AI systems in the AML/CFT sector. The current lack of clear regulation undermines legal certainty for obliged entities and weakens the protection of individual rights. It also appears necessary to strengthen the role of the JFSA by imposing an obligation on financial institutions to report the implementation of high-risk algorithms and to conduct data protection impact assessments (DPIAs) prior to deploying AI solutions. Consideration should also be given to amending the APPI to include provisions on mandatory human participation in decision-making and the right of clients to receive an explanation. An additional step could be the establishment of a regulatory sandbox dedicated to testing RegTech and AI solutions in AML, in cooperation with obliged entities, academia, and technology regulators.

With respect to the European Union, further harmonisation of AI deployment in AML/CFT is recommended, including the development of integrated guidelines encompassing the AI Act, the proposed Anti-Money Laundering Regulation and the GDPR. To this end, it is advisable to establish a specialised working group on AI and supervisory technology (RegTech) within the AMLA, tasked with developing uniform technical and regulatory standards. From a strategic perspective, the EU should also support the development of interoperable scoring tools based on XAI models, which could serve as shared infrastructure for the financial sector across the Union. Such initiatives would enhance supervisory effectiveness while ensuring alignment with EU values regarding data protection and individual rights.

This study points to the need for further in-depth empirical research on the extent of AI implementation and the practical experiences of obliged entities in AML/CFT, with particular attention on supervisory mechanisms and compliance with data protection laws. It would be especially valuable to investigate how human oversight of algorithms is exercised in practice and to what extent financial institutions can ensure the explainability of decision-making models. At the same time, interdisciplinary research should be undertaken to design standards for XAI in the compliance sector, incorporating auditability requirements and data minimisation principles.

It is also warranted to broaden the scope of legal comparison to include other jurisdictions, particularly the United States and Singapore, which are distinguished by their pragmatic

and diversified approaches to the integration of technology into financial supervision. Analyses of these countries could provide further arguments for more flexible or sector-specific regulatory frameworks. Lastly, future research should also include a deeper reflection on the ethical and societal implications of AI in AML systems—particularly the risks of algorithmic exclusion and the impact on public trust in financial systems and public institutions.

Funding

This research received no external funding.

Data Availability Statement

Data sharing is not applicable to this article. No new data was created or analysed in this study. All sources analysed (legal acts, supervisory guidance, and case law) are publicly available and are cited in the References.

Disclosure Statement

No potential conflict of interest was reported by the author.

The author read and agreed to the published version of the manuscript.

References

Alhajeri, R. and Alhashem, A. (2023) 'Using artificial intelligence to combat money laundering', *Intelligent Information Management*, 15(4), pp. 284-305. doi: 10.4236/iim.2023.154014.

Arslanian, H. and Fischer, F. (2019) 'Applications of artificial intelligence in financial services', in *The future of finance: The impact of FinTech, AI, and crypto on financial services*. Cham: Springer, pp. 179–197. doi: 10.1007/978-3-030-14533-0_15.

Article 29 Working Party (2018) Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 rev.01). Available at: https://ec.europa.eu/newsroom/article29/items/612053/en (Accessed: 16 May 2025).

Azzutti, A. (2024) 'AI governance and algorithmic trading: Some regulatory insights from the EU AI Act', *Banking & Finance Law Review*, 41(1), pp. 133–168. doi: 10.2139/ssrn.4939604.

Azzutti, A., Batista, P.M. and Ringe, W.-G. (2024) 'Good administration in AI-enhanced banking supervision: A risk-based approach', *Columbia Journal of European Law*, 29(3), pp. 434–497. Available at: https://cjel.law.columbia.edu/print/2024/good-administration-in-ai-enhanced-banking-supervision-a-risk-based-approach/ (Accessed: 26 September 2025).

Bukowski, M. (2023) 'Combating economic cybercrime using artificial intelligence (AI)', *The Police Review*, 151(3), pp. 151–179. doi: 10.5604/01.3001.0053.9746.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2021) *Big data and artificial intelligence: Principles for the use of algorithms in decision-making processes*. Available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2021/meldung_210615_Prinzipienpapier_BD_KI_en.html (Accessed: 16 May 2025).

Centraleyes (no date) *French data protection act (Loi informatique et libertés)*. Available at: https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf (Accessed: 16 May 2025).

Chancellery of the Sejm of the Republic of Poland (2018) Ustawa z dnia 1 marca 2018 r.o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. *Journal of Laws*, item 723 (Dz.U. 2018 item 723).

Commission nationale de l'informatique et des libertés (CNIL) (2025) *AI and GDPR: The CNIL publishes new recommendations to support responsible innovation* (7 February 2025). Available at: https://www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation (Accessed: 16 May 2025).

Court of Justice of the European Union (CJEU) (2023) *SCHUFA Holding and Others (Scoring), case C-634/21, judgment of 7 December 2023*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A62021CJ0634 (Accessed: 26 May 2025).

Court of Justice of the European Union (CJEU) (2025) *CK v Dun & Bradstreet Austria GmbH, case C-203/22, judgment of 27 February 2025*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62022CJ0203 (Accessed: 26 May 2025).

European Commission (2021) *Money laundering* [online]. Available at: https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/money-laundering_en (Accessed: 16 May 2025).

European Commission (2024) *Anti-money laundering and countering the financing of terrorism at EU level*. Available at: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en (Accessed: 16 May 2025).

European Parliament and Council (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 16 May 2025).

European Parliament and Council (2024a) *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.* Available at: https://eur-lex.europa.eu/eli/dir/2024/1640/oj (Accessed: 16 May 2025).

European Parliament and Council (2024b) *Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.* Available at: https://eur-lex.europa.eu/eli/reg/2024/1620/oj (Accessed: 16 May 2025).

European Parliament and Council (2024c) *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.* Available at: https://eur-lex.europa.eu/eli/reg/2024/1624/oj (Accessed: 16 May 2025).

European Parliament and Council (2024d) *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024.* Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (Accessed: 16 May 2025).

Fan, J., Shar, L.K., Zhang, R., Liu, Z., Yang, W., Niyato, D., et al. (2025) 'Deep learning approaches for anti-money laundering on mobile transactions: Review, framework, and directions', *arXiv preprint*:2503.10058, pp. 1–25. doi: 10.48550/arXiv.2503.10058.

Financial Action Task Force (FATF) (2021a) *Digital transformation of AML/CFT for operational agencies: Detection of suspicious activities and analysis of financial intelligence*. Paris: Financial Action Task Force. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Digital-Transformation-executive-summary.pdf (Accessed: 16 May 2025).

Financial Action Task Force (FATF) (2021b) *Opportunities and challenges of new technologies for AML/CFT*. Financial Action Task Force. Available at: https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html (Accessed: 16 May 2025).

Financial Action Task Force (FATF) (2025) *The FATF recommendations*. Paris: Financial Action Task Force. Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (Accessed: 16 May 2025).

Financial Services Agency (2023a) *Comprehensive guidelines for supervision of financial instruments business operators, etc.* Available at: https://www.fsa.go.jp/common/law/guide/kinyushohin_eng.pdf (Accessed: 16 May 2025).

Financial Services Agency (2023b) *The JFSA strategic priorities July 2023–June 2024*. Available at: https://www.fsa.go.jp/en/news/2023/the_jfsa_strategic_priorities_july2023-june2024.pdf (Accessed: 16 May 2025).

Financial Services Agency of Japan (JFSA) (2025) *AI discussion paper version 1.0*. Available at: https://www.fsa.go.jp/en/news/2025/20250304/aidp_en.pdf (Accessed: 16 May 2025).

French Financial Markets Authority (AMF) (2022) *Annual report 2022*. Available at: https://www.amf-france.org/sites/institutionnel/files/private/2024-05/ra_amf_2022_eng.pdf (Accessed: 17 May 2025).

Generalny Inspektor Informacji Finansowej (GIIF) (no date) *Komunikaty generalnego inspektora informacji finansowej publikowane są na stronie BIP*. Available at: https://www.gov.pl/web/finanse/generalny-inspektor-informacji-finansowej (Accessed: 16 May 2025).

Goodell, J.W., Kumar, S., Lim, W.M. and Pattnaik, D. (2021) 'Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis', *Journal of Behavioral and Experimental Finance*, 32, 100577. doi: 10.1016/j.jbef.2021.100577.

Government of Germany (2017) *Money Laundering Act (Geldwäschegesetz—GwG)*. Available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html (Accessed: 16 May 2025).

Government of Japan (2003) *Act on the protection of personal information (Act No. 57 of 2003)*. Available at: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en (Accessed: 17 May 2025).

Government of Japan (2007) *Act on prevention of transfer of criminal proceeds (Act No. 22 of 2007)*. Available at: https://laws.e-gov.go.jp/law/419AC0000000022 (Accessed: 16 May 2025).

Information Commissioner's Office (ICO) (2020) *Guidance on AI and data protection* (updated 2023). Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection (Accessed: 16 May 2025).

International Organization of Securities Commissions (IOSCO) (2024) *Artificial intelligence in capital markets: Use cases, risks, and challenges*. International Organization of Securities Commissions, pp. 1–31. Available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD759.pdf (Accessed: 16 May 2025).

Kędzierski, M.A. (2023) 'A proposal to use reinforcement learning to optimize decision-making in the field of counteracting money laundering and terrorist financing. Part 2', *Modern Management Systems* 18(4), pp. 49–68. doi: 10.37055/nsz/188842.

Komisja Nadzoru Finansowego (KNF). (2019) *Raport z prac Zespołu ds. innowacji finansowych FinTech*. Available at: https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_z_prac_Zespolu_ds_rozwoju_innowacji_finansowych_73565.pdf (Accessed: 16 May 2025).

Kuiper, O., van den Berg, M., van der Burgt, J. and Leijnen, S. (2021) 'Exploring explainable AI in the financial sector: Perspectives of banks and supervisory authorities', *arXiv preprint*. doi: 10.48550/arXiv.2111.02244.

Légifrance (2025) *Code monétaire et financier—Chapitre Ier: Obligations relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme* (Articles L561-1 à L561-50). Available at: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072026/LEGISCTA000006154830/ (Accessed: 16 May 2025).

Mirishli, S. (2023) 'Ethical implications of AI in data collection: Balancing innovation with privacy', *QƏDİM DİYAR (Ancient Land) International Online Scientific Journal*, 6(8), pp. 40–55. doi: 10.36719/2706-6185/38/40-55.

Organization for Economic Cooperation and Development (OECD) (2021) *Ending the shell game: Cracking down on the professionals who enable tax and white collar crimes*. Paris: OECD Publishing. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/02/ending-the-shell-game_79ff90e4/79e22c41-en.pdf (Accessed: 16 May 2025).

Organization for Economic Cooperation and Development (OECD) (2024) *Regulatory approaches to artificial intelligence in finance*. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-finance_f1498c02-en.html (Accessed: 26 September 2025).

Ozaki, H. (2019) 'AML/CFT and new technologies: Challenges in Japan', *Journal of Financial Compliance*, 2(4), pp. 342–361. doi: 10.69554/DMGV6814.

Ranković, M., Gurgu, E., Martins, O.M.D. and Vukasović, M. (2023) 'Artificial intelligence and the evolution of finance: Opportunities, challenges, and ethical considerations', EdTech Journal, 3(1), pp. 20–23. doi: 10.18485/edtech.2023.3.1.2.

Tracfin (2023) *Tracfin's activity in 2022*. Available at: https://www.economie.gouv.fr/files/files/directions_services/tracfin/TRACFIN_2022_Tome2_EN_Web.pdf (Accessed: 16 May 2025).

United Nations Office on Drugs and Crime (UNODC) (2023) *Money-laundering*. Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html (Accessed: 16 May 2025).

Yeo, W.J., van der Heever, W., Mao, R., Cambria, E., Satapathy, R. and Mengaldo, G. (2023) 'A comprehensive review on financial explainable AI', *Artificial Intelligence Review*, 58, Article No. 189. doi: 10.1007/s10462-024-11077-7.