Remittences Review
October 2022
Volume:7 , No: 2 ,pp.243-258
ISSN: 2059-6588(Print)| ISSN: 2059-6596 (Online)

Received: 22 July 2022, Accepted: 27 August 2022

GLOBAL GOVERNANCE AND TECHNOLOGICAL DISRUPTION: ADDRESSING MONEY LAUNDERING AND TERRORISM FINANCING IN A DIGITAL AGE

GHULAM MUJTABA MALIK1, RASHID WASSAN2, LIAQAT ALI3, JAHANGEER ALI4, SARJEET SINGH OAD5

1.PhD Candidate in Law, Faculty of Law and Political Science, University of Szeged, Hungary. Email: gh.mujtaba@hotmail.com(Corresponding Author)
2.PhD. Scholar, Department of Criminology, University of Sindh Jamshoro, Pakistan
Email: rashid.wassan2k22@gmail.com
3.Mphil Scholar, Department of Criminology,University of Sindh Jamshoro, Pakistan
Email: meliaqat2003@gmail.com
4.Mphil Scholar, Department of Criminology,University of Sindh Jamshoro, Pakistan
Email: Hotz_ice@hotmail.com
5Mphil Scholar, Department of Criminology,University of Sindh Jamshoro, Pakistan
Email: sarjeets346@gmail.com

Abstract

This study explores the evolving challenges and responses associated with money laundering (ML) and terrorism financing (TF) in the context of technological disruption and global governance. It examines the transformation of anti-money laundering and counter-terrorism financing (AML/CFT) regimes under the influence of emerging financial technologies, such as digital currencies, distributed ledger technologies (DLT), and virtual assets. Through a qualitative review of legal instruments, policy guidelines, and scholarly literature, the paper analyzes how criminals exploit technological advancements and regulatory gaps to obscure illicit financial flows. It also investigates the limitations of existing international legal frameworks, particularly about harmonization, enforcement, and risk-based compliance strategies. Findings highlight that while developed countries are advancing with RegTech solutions and digital regulatory tools, developing countries face infrastructural and legislative constraints that hinder AML/CFT implementation. The study also reveals that financial globalization and digital decentralization exacerbate challenges for cross-border cooperation and oversight. Drawing on transparency-stability and systems theory, the research underscores the importance of multilevel governance, legal harmonization, and proactive technological adaptation. The paper concludes by recommending stronger global coordination, enhanced public–private partnerships, and the integration of innovative regulatory tools to strengthen AML/CFT resilience in an increasingly digital financial ecosystem.

Keywords: Global Governance, Technological Disruption, Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), Financial Crime, Money Laundering, Terrorism Financing, Compliance Frameworks, Digital Economy, Financial Regulation

1. Introduction

The global financial system is under serious threat from the rapid advancement in technology-related economic crimes; regulators must adapt to these developments. Technology poses unknowable risks (Zarate, 2020), necessitating new regulations to reduce risks and modify

existing laws. As a result, we may require new laws to mitigate the risks posed by technological developments to globalized crime, including money laundering and terror financing. Money laundering involves Smurfing and Structuring, which entails splitting up significant deposits to circumvent reporting requirements, then entering the financial sector through numerous channels, and lastly entering the actual economy. Because of its ease of flow around the world, digital currency is more difficult to track than tangible currency (Bryans, 2014). It transforms into a line on paper or a computer screen, making it easier for money launderers to deposit enormous sums of money. Digital banking also makes it easier for launderers to perform transactions without having to visit banks or fill out papers, making it more difficult to track down account owners. This paper examines the theoretical and regulatory expansion of anti-money laundering and counter-terrorism frameworks in the context of risks and problems created by recent technological advancements. The purpose of the study is to assess the risks associated with global financial crimes that have spread worldwide, as well as any potential flaws or enhancements that could otherwise act as channels for terrorist and criminal networks. There is a sizable body of literature that discusses the difficulties associated with current AML/CTF laws in place globally in accordance with international standards.This study examines the current challenges posed by advances in money laundering and terrorism in the context of globalization. The finding of this paper suggests that the terrorists need funds and assets so as to arrange for, purchase weapons, travel, and execute crimes (Napoleoni, 2003). Even though criminals may work with genuine companies' geographical gaps might make detection challenge. It can be difficult for smaller groups since they frequently spend meager sums of money. The FATF is a government agency that monitors money laundering (FATF, 2020) and terrorism financing on a global scale and establishes norms to stop and lessen harm.Member states have ratified these standards, and they have been incorporated into national laws, including EU Law, which is based on them. Its recommendations or standards aim to ensure an international response that is consistent to both existing and emerging potential dangers. Meanwhile, several improvements to existing laws could potentially impact new advancements in technology. Additionally, many developed nations have enacted specialized laws addressing technology and new payment methods, in contrast to developing countries. For any new regulatory obstacle, nations have two conflicting strategies. They are free to choose various strategies apart from one another. They can also try to prevent conflicting laws by adopting consistent regulations issued by international organizations like the FATF, which all member countries have broadly embraced.

2. Money Laundering Is A Serious, Illegal Problem, Which Is Why It Matters.

2.1 Understanding Money Laundering: Definitions, Evolution, and Emerging Risks

The primary goal of money laundering is to separate proceeds from their source, a practice that spans over 2,000 years and began in China when businessmen transformed illegal trading earnings into legitimate money(Gelemerova, L. 2011). Criminals have utilized this practice to recycle, conceal, and legitimize their income, allowing them to live a luxury lifestyle while growing their unlawful activity. The Italian and American mafias have also employed money laundering to disguise funds earned through criminal activity. Money laundering is defined by the Financial Action Task Force (FATF) as the processing of criminal proceeds in order to disguise their illegal origin, with international harmonization concentrating on political concerns, organized crime, corruption, economic development, and terrorist financing. Money

laundering is a criminal activity that involves the legalization of illegally obtained funds through a variety of techniques, including drug-related offences, human trafficking, the arms trade, fraud, and corruption. Money laundering, according to Shavirta (2008), Van Duyne (2003), and Alldridge (2003), entails legitimizing illegally obtained proceeds. However, these definitions exclude the electronic and digital avenues used to conceal the source of funds, such as international and local money transfers, and technology-based means, which refer to products and services made available to the financial services industry as a result of technological advancements.

Technology has been developed to circumvent existing legal frameworks, raising concerns about the adequacy of current AML/CFT global legislation, which is based on the FATF 40 guidelines and their implications. The three-stage money laundering method is criticized for being overly simple and overlooking technological money laundering. Money launderers often use financial services to formalize illegal revenues, highlighting their dynamic and ever-changing nature. Technology can either lead to novel solutions or disrupt financial services, requiring new development and disruption standards. However, these changes have the potential to disrupt the heavily regulated sector, allowing money launderers to seize opportunities and jeopardizing the integrity of the financial system. While technology can reduce compliance costs, it also poses risks to privacy and security, as well as jeopardizing the integrity of the banking system. Technological and regulatory shortcomings in the application of AML/CFT legislation continue to provide opportunities for money launderers while undermining the effectiveness of regulations.

Global governance encompasses relations among individuals, countries, markets, and authorities, as well as international shipping and mail. Financial markets, terrorism, climate change, product safety, and food availability are all addressed. However, the benefits of globalization are not evenly dispersed, and regulatory and monitoring mechanisms are still primarily national in scope. Money launderers are increasingly adopting innovative technologies, which is a serious international threat. The interrelation of actions in cyberspace is currently a significant concern to the global community, mostly because of the negative effects it causes that disturbs the financial sector and the global economy. It goes beyond national boundaries and incorporates international criminal activities and sophisticated forms, strategies, and processes. When money is being laundered, especially when it is being layered into the regulated financial system, technology is a major enabler. Financial institutions can analyze transactions and shady activity with the aid of AML compliance software. To manage illicit currency across several deposits or asset conversions or to lessen visibility, money launderers must constantly refine their technique. According to the UNODC data (UNODC, 2011), illicit proceeds excluding tax evasion totaled $2.1 trillion in 2009, or 3.6% of GDP. 1.5% of the world's GDP was made up of the proceeds of transnational organized crime, which includes drug trafficking, counterfeiting, human trafficking, and arms smuggling. 70% of these proceeds were probably laundered through the banking system. The FATF suspects that 2% of the world's GDP, or $1.2 trillion, is laundered annually.The IMFestimates that money laundering accounts for 2% to 5% of worldwide GDP, with illegal proceeds likely totaling 3.6%, or $2.1 trillion.Modernization and digitization of the world economy on a global scale may be advantageous to terrorists, drug traffickers, and dishonest officials, enabling them to launder money through new methods and techniques. According to Europal Director Rob Wainwright, three to four billion pounds of illicit funds are being laundered in Europe (Europol, 2020) via digital currencies. The difficulties brought on by anonymity and a

lack of oversight must be addressed by regulators and industry leaders. Due to their lack of government regulation, anonymous transactions, and convenient cross-border use, digital currencies have advantages but also run the risk of being used for money laundering. Global financial stability is seriously threatened by online money laundering. For example, the most significant online money laundering case, Liberty Reserve (Campbell-Verduyn, 2018), included more than US$6 billion being laundered among over one million users worldwide. Technology helps criminals deposit, move, and use illegal funds obtained through criminal activity. E-commerce and mobile payments are two prominent examples of transaction laundering. The laundering of illegal gains involved a global internet payment service provider, a digital currency exchange, and companies that make stored value cards. Additionally, a criminal organization employed online betting and payment services to launder drugs. The advancement of technology poses challenges to governments and central banks in regulating money and exchange rate policy, as it disrupts payment systems and circumvents regulatory frameworks due to decentralization. Regulators should not only alert the public about the risks of advancements and technology in the financial sector, but also adopt comprehensive international and national regulations for control and administration, as well as upgrade the anti-money laundering framework to address emerging threats.

2.1.1 An Overview of Money Laundering Stages

Placement, layering, and integration are the three stages of money laundering. During the placement stage, illicit monies are injected into the financial system through methods such as structuring, smurfing, money mule transactions, alternative remittance networks, purchasing high-value items, repaying bank debts, and smuggling cash (Unger & Ferwerda, 2011; Cassella, 2018). The layering phase entails transferring funds through complex financial transactions to disguise their nature and location. This process is critical for money launderers because it obscures audit trails and complicates efforts by authorities to trace illicit origins (Reuter & Truman, 2004). In the integration phase, laundered funds are reintroduced into the economy through activities like purchasing luxury assets or investing in legal enterprises. The specific tactics vary depending on the type of crime and the effectiveness of a country's anti-money laundering (AML) system (Gilmore, 2004).

The global financial system depends on the integrity of financial institutions, which are expected to adhere to legal, professional, and ethical standards. Money laundering can significantly damage the reputation of financial institutions and undermine democratic governance and the rule of law (Pol, 2020). Techniques used for laundering money are often the same as those employed to conceal the financial sources of terrorism. For this reason, the Financial Action Task Force (FATF) recommends that jurisdictions criminalize not only money laundering but also the financing of terrorism, including support for terrorist organizations and activities (FATF, 2012). Moreover, recent technological advancements and the globalization of finance have made it increasingly difficult to detect, freeze, and confiscate proceeds of crime (Zarate, 2020; Akartuna, Johnson, & Thornton, 2022).

2.2The Interconnection between Money Laundering and Terrorism Financing

Money laundering and terrorism financing are serious global problems, yet attempts to combat them are insufficient. Money laundering and terrorism funding are significant global economic challenges that jeopardize financial institutions and money flows. Developed governments have established technologically advanced due diligence methods to battle ML

and FT, and emerging markets continue to improve these procedures. Developing countries are striving to limit ML in their financial systems in order to boost economic growth. The uncontrolled economy and unregulated financial discipline have long been barriers to economic progress in developing countries, and the soundness of the country's financial system is closely tied to economic advancement. To address these challenges, shared principles and international cooperation are required(Cornford, A., & Kregel, J. A. 1996), including the implementation of anti-terrorism legislation and the encouragement of new governments to join international treaties. As a result of differing legal norms, these concerns are becoming more challenging to address. Terrorism can have global consequences, and because the globe is interrelated, it is critical to share ideals and collaborate to combat international terrorism. The current section of the study investigates criminals' money laundering and terrorism financing strategies, addressing a lack of awareness about their methods. It investigates how they make money from significant crimes such as offshore vehicles, gambling, derivatives, and forgery.Terrorist financiers, unlike money launderers, can earn both legal and illicit income. The Council of Europe Convention emphasizes the twofold public hazard of money laundering: it hides criminal proceeds from the spotlight while also enabling terrorist actions by investing laundered funds in them (Ghimire, M. 2022). Money laundering and terrorist financing are inextricably linked, with traditional finance derived from illegal activities such as narcotics trafficking. Another trend is the fight against terrorist financing, with Financial Action Task Force (FATF) recommendations focused on suspicious transactions and criminal culpability. This has raised the relevance of money laundering as a prerequisite for financing terrorism, with funds of legitimate origins funding almost half of all acts. Terrorist organizations' money laundering operations are becoming self-sufficient.

In the twenty-first century, the rise of virtual criminals in financial crime has created complex regulatory challenges at both national and international levels. Globalization has necessitated the formation of new governance mechanisms to address increasingly borderless economic and criminal activities (Tsingou, 2010). Early research on money laundering (ML) and terrorism financing (FT) focused on identifying typologies, particularly in medium- to high-risk jurisdictions during the 1990s (Gilmore, 2004). However, the academic focus has since shifted toward the development of legal rules and institutional regulations aimed at preventing financial malpractice (Findlay, 2013). Contemporary studies have broadened to examine the systemic impact of ML/FT on various sectors, particularly emphasizing the role of financial gatekeepers such as banks, lawyers, and accountants in detecting and reporting suspicious activities (Mitsilegas, 2003). In developing and emerging economies, where regulatory infrastructures may be weaker, strong legal linkages and institutional capacity-building are critical to reducing vulnerabilities and preventing manipulative financial behavior (Dobrowolski & Sułkowski, 2019).

To address shared global challenges, new players like the Financial Action Task Force (FATF), along with reformed international organizations such as the International Monetary Fund (IMF) and the United Nations (UN), have taken central roles in the global anti-financial crime agenda. These actors increasingly rely on hybrid regulatory models that combine formal treaties with informal coordination and soft law mechanisms, enhancing the flexibility and responsiveness of governance frameworks (Campbell-Verduyn, 2018; Tsingou, 2010). Terrorist financing refers to the use of the financial system by terrorist groups to fund illegal operations, often originating from criminal activities such as drug trafficking, smuggling, or fraud (Napoleoni, 2003). These funds may either intentionally benefit from institutional

cooperation or be inadvertently facilitated by financial entities that fail to perform adequate due diligence (Reuter & Truman, 2004). As ML/FT networks operate transnationally, concerns have grown about the adequacy of global regulatory frameworks in managing the negative externalities of financial globalization, especially the risk of distorting capital flows and weakening financial system integrity (Pol, 2020).

3. Research Strategy

A qualitative approach was used to study global AML/CFT regulations and applications in the context of the advancement of technology and its challenges. A current literature and document analysis was conducted. The study also analyzed published regulatory enforcements, focusing on transparency, stability theory and the latest developments on the subject, including impactful and innovativeones.

4. Technological Advancements have influenced the Evolution of International AML/CFT Laws

Despite the AML and FATF regulations in force since the late 1980s, money laundering (ML) and terrorism financing (TF) regulation remains an underexplored topic in international law. The anti-money laundering/counter-financing of terrorism (AML/CFT) framework is often characterized as *soft law*, raising concerns about the effectiveness of non-binding international instruments in achieving robust compliance (Gelemerova, 2011; Gilmore, 2004). Nevertheless, the growing legalization of international financial regulation is increasingly tied to states' willingness to adhere to these global standards (Mitsilegas, 2003). Addressing ML/TF effectively requires a dual approach—through international legal instruments and domestic policy implementation. To this end, the G7 established the Financial Action Task Force (FATF) in 1989 to coordinate efforts against drug-related money laundering and safeguard the global financial system's integrity (FATF, 2012). Over time, the FATF expanded its mandate to include counter-terrorism financing, issuing a set of eight (later expanded to 40 + 9) key recommendations. Globalization has catalyzed the emergence of new governance architectures. In this environment, institutions like the FATF, along with reformed entities such as the International Monetary Fund (IMF) and the United Nations (UN), have become pivotal actors in managing cross-border financial threats (Tsingou, 2010). These organizations rely on hybrid mechanisms that combine binding treaties with informal cooperation strategies, enabling flexible and dynamic responses to transnational financial crime (Campbell-Verduyn, 2018).

In addition, non-state actors—such as NGOs, private financial institutions, and public-private partnerships—support trans-governmental regulatory networks in implementing AML/CFT measures (Findlay, 2013). This collaborative infrastructure exemplifies a form of "networked minimalism," wherein national institutions preserve democratic processes while benefiting from supranational guidance on financial regulation (Mitsilegas, 2003). Through such issue-based networks, global governance becomes more accessible and effective, particularly in addressing crimes that transcend borders and leverage digital innovation. The integration of both *hard law* (e.g., UN conventions) and *soft law* (e.g., FATF recommendations) has significantly shaped international AML/CFT frameworks, enhancing legitimacy and compliance (Pol, 2020). Soft law mechanisms often serve as precursors or supplements to legally binding instruments. For instance, FATF Recommendation I calls for the

criminalization of money laundering based on definitions outlined in the 1988 UN Vienna Convention and the 2000 Palermo Convention. Similarly, Special Recommendation II on terrorism financing is aligned with the 1999 UN Convention on the Suppression of the Financing of Terrorism, illustrating the mutual reinforcement of international legal instruments (Gilmore, 2004).

The FATF continues to set global standards for combating ML/TF in cooperation with key regional and international organizations including the UN, the World Bank, and the IMF. In 2004, it adopted five strategic objectives: setting global standards, advancing international engagement, expanding membership, fostering cooperative networks, and promoting research (FATF, 2012). To ensure implementation, the FATF, along with the IMF and World Bank, developed a monitoring framework across nine Financial Action Task Force–Style Regional Bodies (FSRBs) operating in over 100 countries. This structure emphasizes adaptability to local contexts while reinforcing international commitments. Compliance with FATF standards is monitored via three core mechanisms: (1) a self-assessment process by member states, (2) mutual evaluations by peer experts, and (3) the Non-Cooperative Countries and Territories (NCCT) process, which involves publicly identifying jurisdictions that fail to meet FATF expectations (Reuter & Truman, 2004). These systems are designed to encourage convergence, transparency, and accountability in the global AML/CFT regime.

4.1 At the Regional Level

The European Union (EU) has been influential with regard to shaping the anti-money laundering (AML) policies since 1980s. Its strategy has gone through a progression with the implementation of a set of six Anti-Money Laundering Directives (AMLDs) to harmonize the AML practices of the member states (Mitsilegas, 2003; European Commission, 2018). Anyway, the differences still prevail among the member states because they have different domestic legal traditions, intensities of enforcement, and many others. In addition, the EU has formulated its AML establishment in line with the requirements of the Financial Action Task Force (FATF) with G7 countries supporting a high level of compliance in the region especially against countries whose offshore financial centers could potentially be used to arbitrage regulations (Gilmore, 2004; Reuter & Truman, 2004). In the recent times, a few regional bodies have cropped up to conduct dialogue, exchange technical knowledge, and review the AML programs. Among others, these are the European Commission (EC), the Gulf Cooperation Council (GCC), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Financial Action Task ForceStyle Regional Bodies (FSRBs), the Offshore Group of Banking Supervisors (Campbell-Verduyn, 2018; Tsingou, 2010). It is stated that these institutions can offer a lot of help in the process of devising AML strategies that can be compatible with international standards, as well as region-specific elements.

4.2 The AML and CFT Regimes and Recent Advances in Technology

The Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) regime is developing in terms of preventive and enforcement regimes of individual countries, regions, and globally. Such mechanisms refer to sanctions, regulation, and due diligence of customers (CDD) and are to be used to exclude illicit financial activity and support the sorting out of assets (FATF, 2012; Gilmore, 2004). Among the organizations and guiding actors in the reduction of the global AML/CFT environments include the Financial Action Task Force

(FATF), Group of Financial Intelligence Units (Egmont Group), and the United Nations Global Programme Against Money Laundering. Nevertheless, there is still a lack of coordination in the field of law enforcement internationally, especially when it comes to data sharing and joint inquiries, and the cooperation is mainly restricted to such organizations as INTERPOL and EUROPOL (Reuter & Truman, 2004; Findlay, 2013). The development of technology has also made the world financial system extremely interconnected allowing the bad actors to take advantage of the jurisdiction loopholes in those jurisdictions that may have weak or unenforced AML regime (Campbell-Verduyn, 2018; Gelemerova, 2011). This has led to a structural change on covert activities in black-markets markets particularly in the advent of digital currencies leading to anonymous and immediate transfer of money.

To cope with these processes, the FATF provided updated recommendations in 2019 to deal with risks involving virtual assets. These recommendations promote the international collaboration and highlight the need to establish strong action plans in order to prevent money laundering and terrorism financing (FATF, 2019). They require, as well, that Virtual Asset Service Providers (VASPs) adhere to regular AML requirements, such as Know Your Customer (KYC) practices, CDD, and transaction tracking (Akartuna, Johnson, & Thornton, 2022). There has been increased use of sophisticated technologies like machine learning, artificial intelligence (AI), and big data analytics-based compliance efforts to identify suspicious transactions better (Singh & Lin, 2021). However, there are major problems in such technologies integration. Conventional AML/CFT systems are characterized by excessive false positive rates with a range between 95% and 99 percent and lead to ineffective supervision and customer experience (Pol, 2020). RegTech solutions promise that they can mitigate these false positives by up to 55 percent, although they are usually held back by the expensive implementation process, especially with limited resources fintech start-ups have (Buiten, 2019). As such, regulations involving AML/CFT must be dynamic, technologically sensitive and incorporative stakeholder consultation so that these laws stay relevant to digital times. Article 48(3) of this United Nations Convention against transnational organized crime (UNTOC) confirms that this requires the utilization of modern technologies that could be used to deal with money laundering, including cyber-surveillance, using forensic data analysis, and the automation of robotic processes (RPA) in order to fight money laundering as well (UNODC, 2004). Currently, law enforcement agencies could spend a lot of their time in data collection manually. By automating these processes, such as an automated system of monitoring transactions, the investigation could give more attention to more risky transactions, and the reliance on a human element would be minimized, which would increase the efficiency and accuracy of these investigations (Hrga, Capuder, & Zarko, 2020).

4.3 Assessing the Limitations of Current AML/CFT Strategies in a Globalized and Digital Landscape

Money laundering is a complex financial crime typically characterized by three main stages: placement**,** layering**,** andintegration. During the placement phase, illicit funds are introduced into the financial system, often through deposits, cash purchases, or front businesses. The layering phase involves obscuring the source and ownership of the funds through intricate transactions across multiple accounts and jurisdictions, sometimes using shell companies or forged documentation. Finally, the integration phase allows the laundered funds to re-enter the legitimate economy, often through investment in real estate, luxury goods, or legal enterprises (Unger & Ferwerda, 2011; Cassella, 2018). While often presented as a linear

three-stage model, money laundering has become increasingly nuanced, evolving from cash-heavy operations in the 1980s into digital and globalized strategies (Gilmore, 2004). Technological innovation and financial globalization have significantly altered the modus operandi of money launderers. Modern laundering techniques now include **trade-based** money laundering**,** digital payment platforms**,** and cross-border crypto currency exchanges (Reuter & Truman, 2004; FATF, 2019). While cash remains a popular laundering tool due to its anonymity, it is increasingly inefficient and subject to stricter reporting controls. Nonetheless, its use persists in underground economies where formal financial access is limited (Pol, 2020).

Emerging technologies—particularly distributed ledger technologies (DLT)**,** FinTech**, and** new payment systems—present new risks. These systems offer convenience, global transferability, and low transaction costs, making them attractive to money launderers and terrorist financiers alike (Campbell-Verduyn, 2018; Hrga et al., 2020). Virtual currencies, such as Bit coin, are especially vulnerable due to their pseudonymous nature and the lack of consistent global regulation (Zohar, 2015). Criminals also exploit legal loopholes through chargeback fraud, or use crypto currencies to bypass financial thresholds intended to trigger AML alerts (Singh & Lin, 2021). Illicit funds may also be diverted into high-cash venues like casinos, nightclubs, or informal value transfer systems, instead of being funneled back into traditional financial institutions. This undermines regulatory oversight and complicates financial intelligence gathering. As such, enforcement agencies are urged to prioritize identifying perpetrators and predicate offences—such as fraud, corruption, and narcotics trafficking—rather than focusing solely on typologies or laundering techniques (Findlay, 2013; FATF, 2012). A thorough understanding of these links is crucial for the development of a resilient and technology-adaptive AML/CFT framework.

5. The Growth of Technology And The Challenges Associated With ML And TF.

5.1 Understanding Technology and Its Disruptive Role in Financial Crime

Technology, which encompasses industries, computer systems, and applied sciences, represents the practical implementation of scientific knowledge to solve real-world problems. It involves interplay of procedures, systems, and tools, with technical and experimental innovation often driving the development of new products and services (Schwab, 2017). Technology is not purely physical; it also consists of processes or sequences of actions that transform tools or systems to achieve specific goals (Arthur, 2009). This section explores the risks posed by disruptive technologies—particularly financial technologies (FinTech)**,** distributed ledger technologies (DLTs)**,** and digital payment systems—which significantly reshape financial ecosystems due to their superior efficiency, speed, and accessibility (Crosman, 2017). The vulnerabilities associated with these innovations often lie not on the distributed ledger itself but within the network of issuers**,** exchangers, and users interacting with decentralized technologies. Law enforcement agencies and financial institutions increasingly struggle to adapt to the fast-evolving illicit uses of these technologies, especially given the pace at which they are adopted in both legitimate and illicit contexts (Böhme et al., 2015). By relying on unregulated decentralized networks, new technologies also foster the use of machine learning (ML) and automated systems, which complicate the incorporation of these risk vectors into strong Know Your Customer (KYC) and Client Due Diligence (CDD) frameworks (Weimer, 2000).

Although legal digital Payment Platforms are useful in making micropayments and international remittances, they pose a tremendous AML/CFT problem because they are anonymous, offer minimal traceability, and are cross-border enabled (Zwick & Dholakia, 2018). Cryptocurrencies and other virtual assets (VAs) are cheap points of entry into laundering operation and enable layering of funds across jurisdictions with a low regulatory border. The new iterations including atomic swaps can subsequently simplify the exchange of one crypto asset into another without utilizing conventional exchanges, complicating regulatory oversight even more (Conti et al., 2018). The increasing acceptance of VAs in international trade, and the entry of institutional investors into those markets, could do so unwittingly, legitimizing large-scale penetration of the proceeds of laundering. Initial Coin Offerings (ICOs) that sometimes have broken or no KYC systems at all, in fact, provide a method by which criminals can launder their illicit balances into verified financial assets. At this stage, these tokens can be sold out at the open markets after being listed and the entire integration process of the laundering cycle is thus accomplished (Catalini & Gans, 2016).

5.2 Disruptive Financial Technologies: Risks, Innovations, and Regulatory Challenges

Digital, decentralized ledger platforms for small user groups are generally referred to as Distributed Ledger Technologies (DLTs). These platforms function on consensus mechanisms**,** whereby users collectively validate and store transactions without the need for centralized intermediaries (Walport, 2016). A well-known example of DLT is blockchain, which supports crypto currency transactions such as Bit coin and Ethereum. DLT has evolved to facilitate the exchange of diverse digital assets—ranging from utility tokens to digital securities—without requiring oversight from a centralized authority (Tapscott & Tapscott, 2016). However, the concept of the Internet of Money (IoM) is plagued by a lack of terminological consistency across jurisdictions and academic communities. Terms such as *tokens, digital tokens, digital currencies, virtual currencies, crypto currencies, digital assets, virtual assets, crypto assets, digital coins*, and *virtual coins* are often used interchangeably, complicating the development of coherent legal frameworks and enforcement mechanisms (Nian & Chuen, 2015; Houben & Snyers, 2018). New Payment Methods (NPMs)—such as mobile money transfers and prepaid cards—have introduced fresh vulnerabilities into the AML/CFT ecosystem. These tools are particularly popular in low-income and under banked regions, where formal banking access is limited, and regulatory frameworks are still developing (Aron, 2018). Mobile payment systems and in-app transaction platforms allow users to store, send, and receive funds without needing a traditional bank account, creating new avenues for money laundering (ML) and terrorism financing (TF) activities (Zarate, 2020).

Many NPMs also integrate value instruments like crypto currencies, prepaid cards, and tokens tied to environmental or social policies. Such tools are also employed in e-commerce, peer-to-peer trade, mobile markets, which notify the further decentralization of the custody of money and erasing the distinction amid legit and unlawful finance flows (Gates et al., 2016). As these platforms expand, so do chances to make anonymous transactions that do not get captured by template AML tools. FinTech also known as Financial Technology is a wide term that encompasses all the financial services innovations modernizing traditional finance, including robo-advisors, and decentralized lending platforms. Such innovations tend to be re-differentiated into incremental and disruptive technologies, which are determined by the radical shift in business models and regulatory demands (Arner, Barberis, & Buckley, 2016).

One particular sub discipline of FinTech is called RegTech, and its specific intent is on offering a technology solution to enhance the benefits of regulatory compliance like real time transaction monitoring, automated risk profiling, and audit trials. According to the UK Financial Conduct Authority (FCA)**,** RegTech offers a complementary approach to traditional regulatory methods by facilitating agile and transparent communication between regulators and financial intermediaries (FCA, 2015). Although originally tailored for the financial sector, RegTech principles are now being adopted across sectors—including healthcare, education, and energy—as a means to enhance governance and accountability (Gozman, Liebenau, & Mangan, 2018).

5.3 Regulatory and Technological Barriers to Controlling Money Laundering and Terrorism Financing

The dilemma of how to manage financial crime risks remains persistent—even when threats are properly identified. Understanding the causes and nature of risk is a long-standing challenge in regulatory discourse, and the central issue lies in crafting risk mitigation strategies that do not stifle innovation (Baldwin, Cave, & Lodge, 2012). Despite sustained policy attention, governments and financial professionals have struggled to develop adequate regulatory responses to the challenges posed by emerging technologies linked to moneylaundering (ML)and terrorism financing (TF) (Zarate, 2020). Money laundering presents unique enforcement challenges due to the constant adaptation of laundering schemes and the rapid transformation of financial channels. Criminals frequently evolve their methods to bypass detection, while law enforcement efforts are hampered by the complexityof tracing illicit proceeds**,** stringent legal due process, and asymmetric access to financial intelligence (Levi, 2012). In parallel, globalization has removed many regulatory and logistical barriers to cross-border trade and capital movement, contributing to the growing ease with which illicit funds are transferred internationally (Picard & Pieroni, 2020).

The emergence of online transfer of finances- real time payments, mobile banking and peer to peer online payments has made it more difficult. The technologies allow making anonymous, fast, and borderless payments, thus complicating the task of finding, tracking, and interrupting laundering schemes by law enforcers (Teichmann, 2021). Additionally, the globalization of digital crime is also an added complication since investigations across borders are usually hampered due to legal and diplomatic barriers; data acquisition in another country is oftentimes slow or impossible (Sharman, 2011). The rise of Distributed Ledger Technology (DLT) into the financial systems has proven to be a disruptive techno-economic phenomenon, having its regulatory chance and risk aspects (Davidson, De Filippi, & Potts, 2018). Although DLT solutions, including a blockchain-based record of transactions, may increase transparency, their decentralized feature and borderless nature makes them difficult to control through compliance measures and enforcement of regulations (Atzori, 2017). The ensuing world will require polycentric co-regulation, in which the regulatory control is spread across different governance levels to augment flexibility, the transparency of governance and its suitability and efficacy into the Internet of Money (IoM) age (Swan, 2015).

5.4 Regulatory Challenges in Governing Virtual Assets and Financial Technologies under AML/CFT Regimes

Although there is an increased concern in ensuring that virtual currencies (VCs) have global anti-money laundering (AML) regulations, there is still no concerted regulatory code. Majorities within the European jurisdictions have concluded that the exchange of virtual asset (VA) to fiat currency operations ought to be subject to the AML requirements. Nevertheless, the laws in different countries vary in their approaches toward the multiple crypto operations, including VA exchangers, custodial wallet providers, Initial Coin Offerings (ICOs), and crypto-to-crypto and crypto-to-fiat exchanges (Blandin et al., 2020). The ECB was the earliest to deal with VAs, in 2012, when they claimed their anonymity and risk of them being abused to money laundering and financing terrorism (ML/TF) (European Central Bank, 2012). VA activity on EU-wide level has been rather modest but has caused concern demanding regulation evolution. Following revelations in the Panama Papers in 2016, the European Commission has introduced amendments to the Fourth Anti-Fraud Money Laundering Directive (MLD4). The result was the adoption of MLD5 in 2018, broadening obligations to AML a broader scope to VA exchange websites and custodial wallet services (European Commission, 2018). The Commission held that this type of gatekeepers should be included within the scope of AML since they may provide an opportunity to access illegal sources of financing. MLD5 dictates VAs operating crypto-to-fiat-exchanges to adhere to KYC, CDD and reporting requirements. Nevertheless, whilst crypto-to-crypto exchanges are largely unregulated, regulation is inconsistent among Member States and guided by FATF regime as well as national discretion (Zilioli, 2021).

To overcome the risks of VAs, in 2015, the Financial Action Task Force (FATF) released a risk-based guidance, which suggests that entities (which are involved in the process of VCs) should employ strong AML/CFT procedures, such as beneficial ownership verification, due diligence, and monitoring of transactions (FATF, 2015). As of October 2018, FATF has revised their Recommendations to specifically address virtual assets and virtual asset service providers (VASPs) as it requests countries to integrate both into national AML/CFT regimes (FATF, 2019). This is a piece of advice that facilitates cross-border regulation cooperation and encourages VASP licensing to enhance oversight. Still, technological limitations, especially when it comes to digital wallets and recipient address verification, still put a dent in the effort to enforce it. Other policies have been suggested such as having an international register of KYC and beneficial ownership information, augmented with distributed ledger (DL) protocols to enhance traceability and transparency (Houben & Snyers, 2018). However, legal issues concerning digital identity systems as part of AML/CFT implementation include data protection, data privacy, and overreaching of jurisdiction (Zetzsche, Buckley, & Arner, 2020). As a balance between innovation and safety, options such as third-party identity verification and application programming interface (APIs) services are seeking use as an optimal method of reducing ML/TF occurrences in the digital space (Scott et al., 2021).

6Key Findings

This study highlights several critical insights into the intersection of technological innovation and the global anti-money laundering/counter-terrorism financing (AML/CFT) framework:

- **Technological Disruption**: Distributed ledger technologies (DLTs), digital payment systems, and virtual assets (VAs) are increasingly exploited for illicit purposes, particularly due to their anonymity, decentralization, and cross-border reach. These technologies complicate traditional AML/CFT oversight mechanisms.

- **Regulatory Inconsistency**: Jurisdictions exhibit considerable divergence in their treatment of VAs, ICOs, and digital identity systems. This lack of harmonization fosters regulatory arbitrage and weakens the collective global response.
- **Adoption of RegTech**: Regulatory technologies (RegTech) have shown promise in enhancing compliance, particularly in areas such as automated due diligence and transaction monitoring. However, implementation remains uneven, especially in under-resourced regulatory environments.
- **Technological and Legal Asymmetries**: Developing countries remain disproportionately vulnerable to ML/TF threats due to infrastructural and legal limitations. These asymmetries impede the effectiveness of international AML/CFT efforts.
- **Theoretical Insights**: The study draws on transparency-stability theory to highlight the role of information asymmetries in enabling ML/TF, and systems theory to emphasize the multilevel complexity of AML/CFT governance.

7. Conclusion and Future Directions

In an era marked by rapid financial innovation, existing AML/CFT frameworks face profound challenges. This study underscores the need for globally coordinated and technologically adaptive responses to counter the increasing sophistication of financial crime. While technological advancements have expanded financial access, they have simultaneously introduced new vulnerabilities into regulatory systems. The emergence of decentralized financial platforms, unregulated digital asset exchanges, and anonymity-enhancing technologies necessitates a reevaluation of AML/CFT strategies.

To strengthen regulatory resilience, the following priorities are recommended:

- The development of globally interoperable digital identity systems to enhance transparency in cross-border transactions.
- Greater investment in RegTech solutions, particularly in high-risk or under-resourced jurisdictions;
- Harmonization of national legislation by evolving FATF standards, with a specific focus on regulating VAs and NPMs;
- Enhanced public-private cooperation to promote real-time information sharing and compliance innovation.

As ML/TF methods continue to evolve, so too must regulatory and technological counter-measures. Ensuring a balance between innovation and oversight will be essential for safeguarding financial integrity in an increasingly digitized and interconnected global economy.

References

1. Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: A futures-oriented scoping review. Security Journal, 1–36.

2. Alldridge, P. (2003). Money laundering law: Forfeiture, confiscation, civil recovery, criminal laundering and taxation of the proceeds of crime. Hart Publishing.
3. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of Fintech: A new post-crisis paradigm? Georgetown Journal of International Law, 47(4), 1271–1319.
4. Arthur, W. B. (2009). The Nature of Technology: What It Is and How It Evolves. Free Press.
5. Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62.
6. Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding Regulation: Theory, Strategy, and Practice (2nd ed.). Oxford University Press.
7. Blandin, A., et al. (2020). Global Cryptoasset Regulatory Landscape Study. Cambridge Centre for Alternative Finance.
8. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238.
9. Bryans, D. (2014). Bitcoin and money laundering: Mining for an effective solution. Indiana Law Journal, 89(1), 441–472.
10. Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. European Journal of Risk Regulation, 10(1), 41–59.
11. Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change, 69(2), 283–305.
12. Cassella, S. D. (2018). Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete? Journal of Money Laundering Control, 21(4), 494–497.
13. Catalini, C., & Gans, J. S. (2016). Some Simple Economics of the Blockchain. MIT Sloan Research Paper No. 5191-16.
14. Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452.
15. Cornford, A., & Kregel, J. A. (1996). Globalization, Capital Flows, and International Regulation. UNCTAD Discussion Paper No. 161.
16. Crosman, P. (2017). Fintech: Threat or Opportunity? American Banker, 182(121), 1.
17. Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639–658.
18. Dobrowolski, Z., & Sułkowski, Ł. (2019). Implementing a sustainable model for anti-money laundering in the United Nations development goals. Sustainability, 12(1), 244.
19. European Central Bank. (2012). Virtual Currency Schemes. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
20. European Commission. (2018). Directive (EU) 2018/843 of the European Parliament and of the Council. 5th Anti-Money Laundering Directive.
21. FATF. (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.
22. FATF. (2015). Guidance for a Risk-Based Approach to Virtual Currencies.
23. FATF. (2019). Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs.
24. FCA. (2015). Call for input: Supporting the development and adoption of RegTech. Financial Conduct Authority.
25. Findlay, M. (2013). Governing Through Globalized Crime: Futures for International Criminal Justice. Willan Publishing.

26. Gates, B., Morrell, C., & Hern, A. (2016). Digital finance for all: Powering inclusive growth in emerging economies. McKinsey Global Institute.
27. Gelemerova, L. (2011). The anti-money laundering system in the context of globalization: A Panopticon built on quicksand? Nijmegen: Wolf Legal Publishers.
28. Ghimire, M. (2022). Cryptocrime, blockchain, and beyond: Investigating criminals' illicit use of cryptocurrency and exploring law enforcement opportunities.
29. Gilmore, W. C. (2004). Dirty Money: The Evolution of International Measures to Counter Money Laundering and the Financing of Terrorism. Council of Europe.
30. Gozman, D., Liebenau, J., & Mangan, D. (2018). The innovation mechanisms of RegTech. Journal of Management Information Systems, 35(1), 122–145.
31. Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime. European Parliament.
32. Hrga, A., Capuder, T., & Žarko, I. P. (2020). Demystifying distributed ledger technologies. IEEE Access, 8, 126149–126163.
33. Levi, M. (2012). The organization of serious crimes for gain. In The Oxford Handbook of Criminology (pp. 595–622). Oxford University Press.
34. Mitsilegas, V. (2003). Money Laundering Counter-Measures in the European Union. Kluwer Law International.
35. Napoleoni, L. (2003). Modern Jihad: Tracing the Dollars Behind the Terror Networks. Pluto Press.
36. Nian, L. P., & Chuen, D. L. K. (2015). Introduction to cryptocurrencies. In Handbook of Digital Currency. Academic Press.
37. Picard, S., & Pieroni, L. (2020). Globalization and money laundering: An empirical analysis. International Journal of Financial Studies, 8(4), 1–20.
38. Pol, R. F. (2020). Anti-money laundering: The world's least practical policy experiment? Policy Design and Practice, 3(1), 73–94.
39. Reuter, P., & Truman, E. M. (2004). Chasing Dirty Money: The Fight Against Money Laundering. Peterson Institute.
40. Schwab, K. (2017). The Fourth Industrial Revolution. Crown Publishing Group.
41. Scott, B., van Reijswoud, V., & Prinsloo, M. (2021). Digital Identity and AML Compliance in Emerging Markets. GSMA Intelligence.
42. Sharman, J. C. (2011). The Money Laundry: Regulating Criminal Finance in the Global Economy. Cornell University Press.
43. Singh, C., & Lin, W. (2021). Can artificial intelligence, RegTech and CharityTech provide effective solutions for AML and CFT? Journal of Money Laundering Control, 24(3), 464–482.
44. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution. Penguin.
45. Teichmann, F. (2021). Anti-Money Laundering Regulation and Emerging Technologies. Springer.
46. Tsingou, E. (2010). Global financial governance and the developing anti-money laundering regime. International Politics, 47(6), 617–637.
47. Unger, B., & Ferwerda, J. (2011). Money Laundering in the Real Estate Sector. Edward Elgar.
48. UNODC. (2004). United Nations Convention Against Transnational Organized Crime and the Protocols Thereto.
49. UNODC. (2011). UNODC Estimates That Criminals May Have Laundered USD 1.6 Trillion in 2009.

50. Walport, M. (2016). Distributed Ledger Technology: Beyond block chain. UK Government Office for Science.
51. Weimer, W. J. (2000). Cyberlaundering: An international cache for microchip money. DePaul Business & Commercial Law Journal, 13, 199.
52. Zarate, J. C. (2020). Treasury's War: The Unleashing of a New Era of Financial Warfare. PublicAffairs.
53. Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2020). Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172–203.
54. Zilioli, C. (2021). Digital assets and European financial law. European Business Law Review, 32(4), 627–648.
55. Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104–113.
56. Zwick, D., & Dholakia, N. (2018). Consumer subjectivity in the age of financial technologies. Journal of Consumer Culture, 18(3), 412–431.