# FIGHTING FINANCIAL CRIME IN THE DIGITAL AGE

## With special regard to cyber-enabled money laundering

Christoph Wronka, M.Sc., LL.M.

A Thesis by Published Papers Submitted in Partial Fulfilment of the Requirements of Liverpool John Moores University for the Degree of Doctor of Philosophy (PhD)

March 2024

## Table of Contents

## Abbreviations

AI ..... Artificial Intelligence
AML ..... Anti-Money Laundering
AMLD..... Anti-Money Laundering Directive
BaFin..... Bundesanstalt für Finanzdienstleistungsaufsicht
CBDC ..... Central Bank Digital Currencies
CFT ..... Counter-Financing of Terrorism
CNP ..... Card-Not-Present
FATF ..... Financial Action Task Force
FI ..... Financial Institution
FIU ..... Financial Intelligence Unit
FT..... Financing of Terrorism
ECB ..... European Central Bank
ECJ ..... European Court of Justice
GDP ..... Gross Domestic Product
GDPR ..... General Data Protection Regulation
ICA ..... International Compliance Association
ICT ..... Information and Communications Technology
IMF ..... International Monetary Fund
IT ..... Information Technology
KYC ..... Know-Your-Customer
MiCA..... Markets in Crypto Assets
ML ..... Money Laundering
NPPS ..... New Payment Products and Systems
P2P ..... Peer-to-Peer
RegTech ..... Regulatory Technologies
RPA ..... Robotic Process Automation
SDG ..... Social Development Goal
ToFR ..... Trade of Funds Regulation
UNGA ..... United Nations General Assembly
UNODC ..... United Nations Office on Drugs and Crime
VA ..... Virtual Assets
VASP ..... Virtual Asset Service Providers
VC ..... Virtual Currency
WEF ..... World Economic Forum

**Abstract**

In order to effectively combat money laundering and terrorist financing carried out by means of cryptocurrencies and cryptoassets, certain conditions must be met.

First, there must be a sufficient and appropriate regulatory framework within which the necessary counter measures can be taken. Several examples show that this legal framework is not only formed by national and supranational state bodies, but also by rules created in the private sector through self-regulation.

Both regulatory systems are equally limited in their mechanisms of action by data protection law. Money laundering manipulations predominantly, if not as a rule, involve data of the persons concerned, and counter-measures will consequently also have to take these data into account. The question of how to resolve this conflict between the interest of the business sector and society in combating a specific form of financial crime and the interest in protecting individual privacy is, as illustrated by a few examples, being addressed not only by state and private regulators but also by the courts.

On the other hand, it should be noted that legally relevant rules must and can be applied regardless of their character. Despite the existing relatively extensive legal framework, users sometimes have problems from a practical point of view in fulfilling the obligations imposed on them. This concerns financial service providers who need concrete assistance, especially in the context of risk management. It is therefore recommended that this should be offered to them on various points by their trade associations through self-regulation.

Especially in the case of non-transparent cyber-enabled criminal processes, the appropriate organisational structures and technical possibilities must be available to identify them as violations of the law. Only when the criminal structures, i.e. the technical possibilities for abuse and the currently practiced manipulations, are known, can crimes be countered preventively and with repressive means. This concerns not only the financial institutions, but also the administrative or law enforcement authorities and the courts, where often a lack of expertise can be identified. This aspect is not only dealt with in part of this paper, but also in detail in the larger part of the publications compiled in the last section.

**Declaration of original authorship**

The work contained in this thesis has not been previously submitted in support of an application for another degree or qualification of this or any other university or other institute of learning. This thesis contains no material previouly published or submitted for publication by another person except where due references has been made.

Signed: Date: 16.03.2024

(Christoph Wronka)

**Acknowledgement**

I would like to express my appreciation to my Lead Supervisor, Dr Emmanuel Guinchard and Co-Supervisor, Dr Francis Okanigbuan. Their support, guidance and professional advice provided to me throughout the duration of the research has been encouraging and I am very greatful for their assistance.

## Ethical Approval Confirmation

According to LJMU regulations and confirmed by decision of the LJMU Research Ethics Committee, no ethical approval is required for a PhD by publication.

# CHAPTER ONE

GENERAL INTRODUCTION

## 1.1 Introduction

The increasing use of cryptocurrencies and crypto-assets for money laundering (ML) purposes, which is varied in its forms, has become a major economic, social and legal problem across the globe. This has led to the development and review of regulatory measures aimed at addressing these challenges. This thesis examines the challenges, particularly cyber-enabled practices from a technological perspective. It further discusses the development of the regulatory environment governing them and the effectiveness of the regulatory measures. The thesis identifies specific legal areas that place particular demands on the regulators, as examples data protection aspects and criminal sanctions are discussed, with particular focus on the consideration of the regulatory procedures. It is argued in this thesis that the use of self-regulatory measures plays a special role for which corresponding recommendations are given.

The thesis comprises five chapters. This chapter introduces the objective of the thesis. It contains the background to the challenges caused by the use of cryptocurrencies and crypto-assets for ML. In addition, this chapter presents the aims and justification of the research, rationale for submitting the thesis in a publication-based format and the research methodology.

## 1.2 Background to the problem

The financial sector is increasingly vulnerable to financial crime due to the complex nature of financial services. The detection and prevention of financial crime within the financial sector present a task that seems to be practically insurmountable due to the oftentimes complicated nature and structure of financial services (Burnes et al., 2017). The threats come from insiders within a financial institution, domestically within a country, and internationally from other countries (Albayati, Kim and Rho, 2020). Criminals could originate from inside the organisation, or they might come from somewhere else entirely (Masciandaro, 2017).

To a large extent, some seven categories of individuals can be identified, who engage in a variety of illegal financial activities. One of the groups includes organised criminal organisations such as terrorist groups who are increasingly resorting to the commission of large-scale frauds for the purpose of funding their activities (Rider, 2015). Another, rather political category, involves corrupt heads of state who abuse and exploit their positions and abilities to loot their nations, which are in most cases already struggling economically (Horton, 2019). At the level of business corporations, senior executives and business leaders are also often seen to engage in financial crime where they manipulate and falsify financial information to give the misrepresented impression that their organisation is in a better financial condition or position than it really is (Altikriti, Nedelec and Barnes, 2022). The most senior employees all the way down to the most junior employees are also studied as well as investigated as the fourth category of people who steal money and other corporate assets. Financial crime may also be committed against an organisation from the outside by a client, a supplier, a contractor, or even by an individual who has no relationship to the organisation at all (Kranacher and Riley,

2019). A growing number of cases include an outside fraudster working in conjunction with an employee to facilitate the achievement of even larger and more favourable outcomes with less effort (Masciandaro, 2017). One last category of individuals who have committed a financial crime is that of the individual criminals who have been successful, as well as the habitual or opportunistic fraudsters who are currently in possession proceeds gained from financial crime (ICA, 2022).

Increasingly, criminals from both within and outside the organisation and country are teaming together more to execute large acts of crime involving money (Altikriti, Nedelec and Barnes, 2022). According to a study by the United Nations Office on Drugs and Crime (UNODC), the estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or 800 billion - 2 trillion US dollars (UNODC, 2022); in the UK alone, the ML volume is said to be 4.3% of GDP equating to £87.9 billion (Aguiar, 2022), in Germany £51.3 billion (Leonards, 2022).

However, “due to the illegal nature of the transactions, precise statistics are not available an it is therefore impossible to produce a definitive estimate of the amount of money that is laundered every year” (FATF, 2024). Methods such as case studies, proxy variables, or models for measuring the shadow economy all tend to under- or overestimate money laundering (Walker and Unger, 2012).

The Financial Actions Task Force (FATF) therefore does not publish any figures in this regard (FATF, 2024). Consequently, the FATF UK mutual evaluation report from 2018 and the follow-up report from 2022 also do not contain any information on the amount of money laundering for the reasons mentioned above (FATF, 2018a, 2022a).

The dramatic development, rise in functionality, global adoption, and significant investment in the recent blockchain and cryptographic technologies and related financial payment products, services, infrastructure, and systems has continued posing significant challenges for monetary policy makers, regulators, and supervisors. Particularly, since cryptocurrencies sprung to life in 2008 with the launch of Bitcoin, fraudsters, hackers, and other criminals have exploited and misused them for various financial crime-related activities, chief among them being ML and financing of terrorism (FT) (Books, 2021, Huang, 2021). With the increasing use of cryptocurrencies, the potential for abuse grew further. Within one year, the number of ML suspicious activity reports received by the German FIU – the national central office for transaction investigations – more than doubled (2020: 2.050, 2021: 5.320) (FIU, 2022).

Cryptocurrencies offer unique payment infrastructures and software protocols that include transmission of convertible cryptography-based value through decentralised peer-to-peer (P2P) pseudo-anonymous computer networks. Many policy makers, regulators, and financial institutions (FIs) globally are increasingly acknowledging the growth of cryptocurrencies. They consider cryptocurrencies as the likely future of monetary transactions and a growing platform for criminals to store and move illicit funds. The sanction-evasion and other illegal activities of these criminals create unique challenges for anti-money laundering and counter financing of terrorism (AML/CFT), including other associated risks (Aggarwal and Kumar, 2021).

Criminal and malicious insiders and outsiders are ready to test and exploit potential vulnerabilities aided by the reality that information technology systems are the ubiquitous mechanism providing access to money (Baesens, Höppner and Verdonck, 2021). Because cryptocurrencies assume a trans-jurisdictional nature, meaning they are borderless, the risks

associated with them, including ML/FT risks, have become a major concern for regulators (Kshetri, 2021), too.

Despite the challenges regulators are facing, it should be noted that the climate has become difficult for FIs, too, who are now increasingly demanded to comply with a complex worldwide network of AML/CFT regulations (Ardizzi, De Franceschis and Giammatteo, 2018; Goecks et al., 2022). Just within the realm of digital currencies alone, international organisations as diverse as the World Bank, the International Monetary Fund (IMF), the Financial Action Task Force (FATF), the European Central Bank (ECB), and the Committee on Payments and Market Infrastructures have all stepped in, often with concerted effort, and offered expert knowledge and guidance on how to mitigate the financial crime risks that are presented by transactions using digital platforms and currencies, noting that the consequences of these risks can be severe (FATF, 2018b; Balani, 2019; Turki et al., 2020; World Bank, 2022).

### 1.3 Research aims and objectives

The aim of this research is to examine the extent to which existing rules, measures, and techniques for combatting cyber-based ML appear to be adequate in addressing the problems identified above. Further to the aim of the research, it considers whether the current regulatory measures should be revised. Further it considers whether additional legal interventions are needed to deal with certain challenges relating to the problems of financial crimes identified in the research.

The research focuses on selected problem areas. These include

i. the methods concerning crypto-business specific risk assessment as well as the State prosecution of cyber-enabled assaults

ii. the regulatory systems: state and private regulation

iii. the relevance of data protection regulation

iv. and IT-supported processes for monitoring cyber-based transactions and the detection of anomalies

The discussion of these points requires not only the consideration of the legal, but also includes a look at the technological framework. In other words: Combatting the misuse of digital currency for fraudulent and other illegitimate purposes is done with legal means as well as technological tools.

Therefore, this research investigates how the information technology used in the mitigation and detection of cyber-enabled financial crime and ML is devised and utilised to identify, organise and characterise financial transactions, as well as the potential for using digital anomaly detection approaches to achieve this objective.

Since its founding, the FATF has championed the utilisation of technology to identify and typify financial crime particularly related to ML and FT (FATF, 2022b). It is possible to gain insight into the financial behaviours of those who are engaging in illegal activity by processing the electronic traces and digital footprints left behind by their financial transactions (besides the direct cash transfers) (Sullivan, 2015). These traces can even be used to prove criminal associations if the transactions are not made directly with cash (Goede, 2012), i.e., by using cryptocurrencies.

In order to accomplish the aim of the study, a socio-technical viewpoint is employed. This perspective calls for researchers to take into consideration not only the technical aspects of information technology systems (e.g. machine learning, big data, regulatory technologies and artificial intelligence), but also the social environment in which these systems are designed and utilised (Loebbecke and Picot, 2015; Markus and Topi, 2015; Priebe and Markus, 2015; Trujillo et al., 2021). In so doing, it is possible to move beyond a discussion of the potential of the technology component of these digital solutions and programs to financial crime, and begin to unravel the variety of social factors, which may support or hinder the performance of the IT and systems solution (Zhang and Trubey, 2018). In particular, the research identifies the technical aspects of adopted approaches to fighting financial crime in the digital age using technology, as well as the social behaviours directly affecting the use of the digital solutions (Pinto and Sobreiro, 2022). In this way, it is possible to determine how an approach to fighting cyber-enabled financial crime and ML powered by technology can be effectively applied (Turki et al., 2020; Varga, Brynielsson and Franke, 2021; Ho, Ko and Mazerolle, 2022; Pinto and Sobreiro, 2022).

The challenges and concerns that have been voiced in connection with the use of IT for the detection of financial crime are similar to those that have been voiced regarding the use of this technology in a broader sense (Chau and Nemcsik, 2020). For example, a significant number of senior managers are concerned about their organisations' lack of expertise in managing big data (Merendino et al., 2018), and a great number of businesses are delaying the implementation of artificial intelligence (AI) because they do not fully understand how it can benefit their organisations (Bughin, Chui and Manyika, 2017). In a similar vein, there is a greater

awareness of the risks that technology poses to individual users, organisations, and society (Saleh, Boujarwah and Al-Dallal, 2001; Stripling et al., 2018; Ariyaluran Habeeb et al., 2019). However, the use of IT is essential for fighting financial crime in the crypto space.

The results of the research conducted are important as they address the challenges that lie at the core of today's digital society. The pervasiveness of financial crimes in the digital age, and the attendant AML/CFT technologies regimes curb cybercrimes as well as the breadth and depth of the impact they have on people's lives on a daily basis. Diakopoulos (2014, p.399) referred to them as "the innovative power players in society" and encouraged scholars and researchers to investigate the origins as well as the "curvatures of that power" as algorithms regulate multidimensional aspects of human lives, and the delineations of their influence can prove difficult to clasp.

### 1.4 Justification of research

Today's global information systems and technology infrastructure has opened up an infinite number of possibilities and opportunities for individuals, groups, business organisations, governmental and intergovernmental agencies to engage in social, economic, legal, political and other human activities (Ahmad et al., 2019; Ariyanto et al., 2021). However, cybercriminals are increasingly targeting and attacking this newfound digital space with precision and sophistication at an alarming rate. Researchers (Canhoto, 2021b; Wessels et al., 2021; Ho, Ko and Mazerolle, 2022) and practitioners (INTERPOL, 2021; Deloitte, 2022; FATF, 2022c; ICA, 2022; World Bank, 2022) have recommended the application of the socio-technical perspective in understanding and implementing interventions and programs for fighting cyber-based financial crime. This research sets out to investigate whether and how socio-technical

approaches including AML regulatory regimes (sociological) as well as machine learning and AI (technical) can assist in fighting cyber-enabled and cyber-related financial crime and contribute to achieving enhanced cyber-risk management and cybersecurity programs. Emerging research (Zhang and Trubey, 2018; Severino and Peng, 2021; Tertychnyi et al., 2022) and expert evidence (Markus and Topi, 2015; Zimiles and Mueller, 2019; FATF, 2022c) point to a lack of understanding and adequate empirical investigation regarding organisations' perceptions and actual use of AML regimes, machine learning algorithms and AI.

### 1.5 Rationale for submitting the thesis by published papers

Being professionally involved in the use and abuse of cryptocurrencies and crypto-assets for many years, the researcher also came into contact with numerous aspects of ML. These experiences have led to the discussion of different problems in several journal articles. They not only deal with the topic from a technological perspective, but also take into account the development of the regulatory environment governing them.

In particular, the increasing use of cryptocurrencies and crypto-assets for ML purposes has become a major economic, social and legal problem.

As the ingenuity of criminals in discovering new technological ways to carry out their schemes grows, so do the requirements for developing countermeasures. In addition to the use of cyber-technical tools these include effective and enforceable legal provisions.

The six articles (see Chapter 5) that form the basis of this thesis examine some of the problems from different viewpoints including the legal-political perspective.

The findings and analysis in the articles are intended to contribute to further penetration of the phenomenon of digital ML processes in scientific and practical aspects. By choosing this format, the researcher also wanted to disseminate the findings, conclusions and recommendations from the articles to the academic community and practitioners in a timely manner.

### 1.6 Research methodology

The researcher adopted a qualitative approach involving doctrinal legal research (as defined by Mann, 2017). The methodical process of doing doctrinal legal research involves carefully reviewing key legal sources such as cases, statutes, and regulations (Taekema, 2021). This approach aims to evaluate the effectiveness of current legal frameworks and regulatory paradigms when used to combat financial crime in the digital age. As presented by Hutchinson (2013, p.15), the method also explores the nuanced aspects of cyber-centric machine learning and the conceivable role of non-state regulating systems. This study approach focuses on a descriptive dissection, drawing knowledge from legal documents and technical expertise. It seeks to understand how established legal principles interact with the changing environment of cryptocurrencies, ultimately advancing a sophisticated comprehension of how to effectively stifle ML in the crypto space.

#### 1.6.1 Identifying and Analysing Legal Sources

The process of identifying and gathering pertinent fundamental legal documents is part of this doctrinal inquiry's initial step (Liebetrau, 2022). This includes an examination of national and international laws, including statutes, rules, and legal precedents (Afzal & Asif, 2019). The researcher reviews and analyse legal rules and regulations created to address the complexity of cyber-enabled ML.

The research process embraces an analysis of the legal system's precise definitions, the penalties for infractions, the procedural rules and the elements that make up offences that apply in these situations. Additionally, a review of relevant law cases is conducted to identify judicial explanations and judgments that are appropriate to instances of cyber-enabled ML. This approach supports the understanding of the legal environment around ML in the crypto space, providing a basis for discussion of necessary legal expansions.

### 1.6.2 Data Analysis Methods

To evaluate legislative necessities and their effects, this research makes use of qualitative data analysis, which is different from quantitative procedures, which use numerical data (Dawadi et al., 2021). Through an emphasis on textual content, qualitative analysis enables the researcher to collect information from the subtleties of legal terminology and interpretation. The following steps are included in the data analysis:

#### 1.6.2.1 Categorisation

The researcher needs to categorise legislative rules and case law according to their importance in preventing ML (Taekema, 2021). These classifications cover questions of jurisdiction, enforcement strategies, and related penalties. Each topic goes through a process of systematic analysis, revealing underlying patterns and new trends. This endeavour enables an understanding of the role that legal frameworks and court rulings play in the battle against cyber-enabled ML, assisting in the creation of more potent countermeasures to this evolving type of financial crime.

#### 1.6.2.2 Interpretative Analysis

To understand the guiding principles and goals of law, the researcher does an interpretative examination of legal texts (Dawadi et al., 2021) Examining legislative intent, precedent-setting decisions, and pertinent legal theories are necessary for this. The objective is to ascertain the justification for particular legal rules and how they relate to crypto-enabled ML.

#### 1.6.2.3 Technical Understanding

The incorporation of technical knowledge is an important component of data analysis. For determining the viability and efficacy of legal measures, it is crucial to comprehend the technical procedures of cyber-enabled ML (Yaacoub et al., 2020). The researcher takes into account technological insights to assess the applicability of enforcement tools and the likelihood that offenders will evade them.

### 1.6.3 Search terms and research period

The search terms which were used for the research were in particular the following: Money laundering, terrorist financing, fraud, financial crime, data protection, GDPR, EU regulation, statutory law, self-regulation, co-regulation, bank, banking, financial institution, financial services, fintech, FATF, crypto assets, cryptocurrency, blockchain, distributed ledger technology, artificial intelligence, big data, cyber security, cyber thread. The majority of scholary references which were used were published within the last 10 years.

## 1.7 Limitations/weaknesses of the research

The research deals with a constantly evolving topic. As the number of new publications on the topic of crypto-regulation that appear almost daily also shows, an assessment of undesired business behaviour can only be made for the moment and with a limited validity in time. This

does not mean that fundamental legal statements and regulations are not valid over a longer period of time, but the practical possibilities of application, e.g. criminal forms of commission, are subject to continuous factual development and corresponding changing legal interpretations. It is a fact that regulations often lag behind developments and thus prophylactic regulatory measures mostly cannot be adequately designed.

## 1.8 Outline of the thesis

Following the introduction Chapter, Chapter 2 contains an overview of the regulatory framework regarding ML and the legal challenges for the regulators when dealing with cyber enabled financial crime. Chapter 3 presents various scholarly viewpoints on ML and the risks and opportunities of using modern technology and how to effectively combat financial crime by using these technologies. Chapter 4 concludes with the findings and recommendations of the study followed by the published articles on various aspects of combating financial crime in the digital age in Chapter 5.

## 1.9 Conclusion

The increasing use of cryptocurrencies has caused major changes in the field of financial services. Criminals are trying to use these currencies for illegal purposes with increasingly sophisticated means. ML and its intended financing of terrorism not only harm individuals and institutions but threaten the financial economy worldwide. The damage caused by criminal activities has now reached an enormous level and continues to increase dramatically. National and supranational efforts are not preventing the growth of damaging acts. Current regulatory measures to combat this are inadequate. The deficits are not only due to a lack of legal measures, but also to a lack of possibilities to recognise criminal activities, because the

personnel, financial and organisational prerequisites for appropriate preventive and repressive measures are not given.

The thesis follows a qualitative and doctrinal legal research approach. The doctrinal research technique used in this thesis allows an in-depth review of legal rules and regulations and how they are used to combat crypto-enabled ML. The researcher examines primary legal sources using descriptive analysis to identify the strengths and shortcomings of the regulatory framework. Methods for qualitative data analysis that allow for subtle insights and a comprehensive understanding of the legal system include classification, comparison analysis, and interpretative analysis. Technical expertise is integrated to guarantee a comprehensive assessment of regulatory effectiveness and potential evasion strategies.

The research focusses of four main problem areas. These include methods concerning crypto-business specific risk assessment; state and private regulation; data protection problems and IT-supported processes for monitoring cyber-based transactions.

## CHAPTER TWO

REGULATORY FRAMEWORK

### 2.1 Introduction

The answer to the question of whether the existing legal framework is sufficient for successfully combatting ML or whether additions are necessary resp. desirable, first requires a brief description of the current regulatory environment.

This chapter therefore outlines the observations and questions derived from this finding, which concern

i. the groups affected and the interests endangered by ML

ii. the typology of regulators

iii. the character of regulatory measures

iv. specific challenges for regulators and law users

v. regulatory weaknesses and potential for improvement

The fight against ML has long been regulated not only by national laws, but is also an international concern due to its cross-border nature. One example are the various initiatives of the European legislative bodies. On an European level the relevant EU-institutions – i.e. the Commission, the Council and the Parliament – deal with the subject mainly in the way of EU-Directives and EU-Regulations, such as

i. the Directives (EU) 2019/843 and 2018/1673 on the prevention of the use of the financial system for the purpose of ML or FTand on combating ML by criminal law – the so-called 5th and 6th Anti-Money Laundering Directives

ii. the Proposal for a revision of the EU Transfer of Funds Regulation (ToFR –COM (2021) 422 final)

iii. the Proposal for a regulation on Markets in Crypto-assets (MiCA –COM (2020) 593 final)

Some of these European legal acts apply directly while others have to be implemented into national law. Even if their focus may differ, their goal is always the same: The fight against ML through prohibitions and requirements at all legal levels.

### 2.2 Injured parties, areas of law affected

Fighting cyber-enabled financial crime is certainly in the interest of various parties directly concerned. The "honest" customers of financial service providers expect that their business relationship will not be used by criminals to harm them. "Identity theft", for example, is a form of intrusion that is intended to enable criminal transactions. Bank clients can come under suspicion of involvement, apart from the risk of losing their own deposits by criminals hijacking financial transactions. Financial service providers are interested in defending themselves against criminal attacks because they do not want to become a target of law enforcement agencies or supervisory authorities in their capacity as accomplices any more than they want to be seen as unreliable in the hard competition with their business rivals and running the risk of losing reputation.

The State, on the other hand, fights cyber-enabled financial crime among other things, because of possible tax evasion, its obligation to prevent and prosecute violations of the embargo regulations under European law 881/2002 (EC), 2580/2001 (EC), 753/2011 (EU) – and of course to protect the national and international financial systems.

Appropriate defuse and protection measures as well as conceivable sanctions must take these different interests into account.

### 2.3 State and private industry regulations

Combatting ML can be achieved in two regulatory ways. It can either be done on a voluntary basis with self-binding rules of the financial industry. Or the state can mandate compliance with certain standards via legislation and administrative means and impose sanctions on non-compliance in various ways.

The approach of adopting regulations on a voluntary basis as “soft law”, whether in the interest of the companies or the industry or in the interest of third parties, is certainly being pursued in many business-sectors. The area of financial services, however, deserves special attention, as the EU-Commission – contrary to occasional critics (Wahlers, 2011) – has expressed reservations in this regard (EU-Commission 2015). Critics point out that this negative stance contradicts a liberal understanding of the state in terms of economic policy. Furthermore, it also disregards the “principle of subsidiarity” derived from the (German) constitution (Wahlers, 2011, p.152). This principle states that the state must always prioritise private self-regulation and may only intervene itself if this approach is unable to achieve the goal desired by society (Isensee, 2001; Frenz, 2001). Shortcomings in monitoring compliance with the rules should not per se speak against private regulation as such. Presumably, the lingering failures of the

financial sector that led resp. contributed to the global financial crisis of 2007/2008 were decisive for the EU-Commission's reservations about self-regulation of this business sector (Wronka, 2020). However, fundamental criticism of the system without differentiating between its contents is not appropriate. Moreover, the very positive development of this regulatory mechanism in recent years, especially in the UK, shows that the reservations cannot be maintained. Details, in particular with regard to the situation in the UK, are discussed in chapter 4.

### 2.4 State regulation

In principle, the fight against cyber-enabled ML is carried out in regulatory terms on four levels, namely through prevention, detection, prosecution and sanctioning of criminal activities. The preventive aspect plays a dominant role, which is also made clear in the explanatory memorandum to the 5$^{th}$ AMLD (OJ/L156/43 (June 2018), Recital 2). In all respects, the regulator must not be able to identify which technical application possibilities are already being used. It must also, where possible, take future practices into account for reasons of legal certainty, considering that the inventiveness of criminals is a major challenge in this regard.

The State can recognise the need for regulation with regard to combatting illegal practices in the use of cryptocurrencies in different areas of law, which are demarcated against each other. Regulatory measures can be based on civil law, administrative law or criminal law. Examples of such measures include the following:

i. The verification of the existence of the conditions for the termination of the contractual relationship existing with the customer by a distrustful financial service provider is carried out from the civil law point of view.

ii. The legality of the denial of a service provider's licence is to be assessed according to administrative law standards.

iii. Criminal justice is responsible for punishing fraudulent conduct and other offences.

The type and density of regulation varies among the EU-countries. Harmonisation and gap-filling are sought, in addition to national initiatives, by means of regulations, directives or recommendations, i.e., legal instruments which are established according to procedural rules under European law and differ in their effects. In view of the nature of the cryptocurrency-business, which is not bound by national borders, the most comprehensive possible standardisation of the law would appear to be desirable, although this should not per se exclude regulatory reservations for national regulators. The question of the competences of courts and authorities is of major importance, too.

### 2.5 Industry self-regulation

There is no uniform understanding of the term private self-regulation in the literature. Rather, one finds a multitude of definitions with different emphases (Wahlers, 2011, p.35). It is predominantly assumed to be a system of rules that safeguards the private and/or public interests, which comes into being through the instruments of civil law or through legally non-binding but de facto normatively binding elements (Langhart, 1993, p.91; Nobel, 1987, cited in Dafour, 1987, p.444). Self-regulation refers to those rules that could often just as well be issued by a State body but are established by organisations that are not part of the State administration (Roßkopf, 1999, p.38; Schwark, 1979, p.218). Associations and federations of the FIs can set standards for legally compliant conduct, the observance of which provides its members with a high degree of legal certainty. One of the strongest arguments regularly cited

for the use of self-regulatory mechanisms is that it relieves the burden on the State (Schwark, 1979, p.218; for further benefits see Wronka, 2020). Moreover, the efficiency of self-disciplinary rules is pointed out, especially, if their observance is in the own interest (von Hippel, 1992, p.98; Frenz, 2001, p.64; Bachmann, 2006, p.54) or for the benefit of those, who are committed to them. These benefits can include, for example, the prophylactic avoidance of violations of the law sanctioned by the State as well as competitive advantages (higher reputation, commercial respectability etc.) over competing market participants, who do not follow the rules.

### 2.6 Prominent regulatory topic: data protection

It is not surprising that, with regard to ML and the fight against terrorism, the ToFR and numerous other – state and self-regulatory – acts emphasise the processing of personal data and its legally guaranteed protection repeatedly. After all, there already exists – in addition to national regulations – a whole series of EC/EU-Regulations and EU-Directives that relate to this area. They include Regulations No 881/2002 (EC), No 2580/2001 (EC), No 753/2011 (EU); Directive No 2015/849 (EU). They require financial service providers to take action in relation to the handling of personal data as part of a risk assessment (cf. Articles 5, 10 and seq. of the German Money Laundering Act; they are based on the FATF's "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" – for details see Gola and Wronka, 2018). These actions include the screening of customers when contracts are concluded, comparison with international and European sanctions lists, and the monitoring of anomalies in transactions.

### 2.6.1 Data processing: permission principles

In most cases the EU-General Data Protection Regulation (GDPR) must be used to assess the legality of data processing. Its basic Article 6 GDPR contains a fundamental prohibition of the processing of personal data in conjunction with a catalogue of exceptions. These concern, for example, data processing that is necessary for the purpose of fulfilling contracts or legal obligations. Furthermore, processing is permitted for the purpose of safeguarding the legitimate interests of the data subject, unless these interests are overridden by the legitimate interest of other persons. Only if one of these in total 6 statutory exceptions can be applied to a specific intended (administrative or legislative) activity, the processing requiring that action is allowed (Schulz, 2018, cited in Gola, 2018; Frenzel, 2018, cited in Paal and Pauly, 2018; Schmid, 2020, cited in Maume and Maute, 2020). It should be added that the EU-principles referred to also apply in the UK, as they have been implemented in UK law via the UK-GDPR and the Data Protection Act 2018.

In other words, a regulator – this can be a legislator but also an authority that issues specific administrative regulations or administrative acts – cannot simply prescribe – perhaps perfectly reasonable – measures that it has not previously checked against the data protection requirements. Rather, the regulator must carefully weigh different legal interests – e.g. balance individual privacy vs. State security interest or economic freedom of action – in the way that stands up to judicial scrutiny. The same applies to private entities such as financial service providers, for example, when customer and transaction data is shared and compared between them.

### 2.6.2 Examples

Three examples will be used to illustrate the interrelationship of the legal regimes concerning ML and data protection respectively the conflict of the different underlying interests, namely on the one hand the efficient fight against ML demanded by society and on the other hand the guarantee of individual data and privacy protection. The first example concerns a case from recent EU-jurisdiction, the second concerns a somewhat older judgment by a national court and the third refers to recommendations by the FATF.

#### 2.6.2.1 European Court of Justice

Of far-reaching importance for the relationship between AML measures resp. the legal provisions on which they are based and data protection requirements is the judgment of the European Court of Justice (ECJ) of 22 November 2022 (ECJ, 2022). The court had to rule on an action brought by two companies against Luxembourg Business Registers for its refusal to limit the general public's access to information on their beneficial owners in the transparency register. In the judgment, the ECJ invalidated Directive 2018/843 of 30 May 2018 (the so-called 5$^{th}$ AMLD 2018), on which the dispute was based, to the extent that it gave the public unrestricted access to such information. According to the ECJ, the unrestricted access constitutes a disproportionate and thus unjustified interference with the right to respect for private and family life protected by Article 7 of the EU Charter of Fundamental Rights and the right to the protection of personal data enshrined in Article 8 of the Charter (judgment, paragraph 88).

The 5th AMLD amended and supplemented Directive 2015/849 of 20 May 2015 (the so-called 4th AMLD) and allowed with the first subparagraph of Article 30 (5) - in addition to individual bodies listed in lit. a and b - access to the information in question to persons and entities that can demonstrate a 'legitimate interest' (lit. c). The 5th AMLD abolished the 'legitimate interest' access barrier. It modified Article 30 (5), first subparagraph, lit. c to require Member States to ensure that information on the beneficial owners of companies and other legal persons is accessible to all members of the public in all cases.

The ECJ recognises the intention of the Directive and the transparency register to prevent the EU financial system from being used for ML and FT (judgement, paragraph 55). This is an objective that serves the common good and can, in principle, justify serious interference with Articles 7 and 8 of the EU Charter of Fundamental Rights (ibid., paragraph 59). In order to satisfy the criterion of 'necessity', however, the interventions must be limited to what is absolutely necessary „in the sense that the objective could not reasonably be achieved in an equally effective manner by other means less prejudicial to those fundamental rights of the data subjects“ (ibid., paragraph 66); this requirement is not met by unrestricted access to information. Moreover, the opening of unrestricted access does not meet the requirement of ‚proportionality‘: „An objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the right at issue, in order to ensure that the disadvantages caused by that measure are not disproportionate to the aims pursued“ (ibid., paragraph 64).

#### 2.6.2.1.1 Effect of the judgment

The invalidation pronounced in the judgment relates solely to the amended Article 30 (5), first subparagraph, lit. c (opening to "all members of the public"). It binds all Union institutions and national law practitioners and applies retroactively (ex tunc; Deutscher Bundestag, 2023). Currently, Article 30 (5), first subparagraph, lit. c of the 4th AMLD is relevant again.

If national law does not comply with this, the relevant provisions must first be interpreted in conformity with EU law or remain inapplicable (Deutscher Bundestag, 2023). In addition, national law that is incompatible with Union law must be adapted in order to avoid legal uncertainty (ECJ 2001; Wegener, 2022; Deutscher Bundestag, 2023). Several countries suspended the allowance of access requests by ‚members of the public' immediately after the judgment was pronounced (Ernst & Young, 2022), e. g. Luxembourg, the Netherlands, Austria or Ireland (Oppenhoff, 2022).

#### 2.6.2.1.2 Impact on the UK register of People with Significant Control (PSC)

Having left the EU, the UK is not bound by the judgement. The ruling was based on the partial incompatibility of the 5th Money Laundering Directive with Articles 7 and 8 of the EU Human Rights Charter. However, the Charter is also no longer applicable to the UK. Even though the UK, which has implemented the 5th Money Laundering Directive with the Money Laundering and Terrorist Financing (Amendment) Regulation 2019 into national law, is not obliged by the ECJ judgment to take further legislative steps, the following should be taken into account:

It should be noted that the rights enshrined in Articles 7 and 8 of the EU Charter are also found in Article 8 of the UK Human Rights Act 1998 in a modified form - incidentally with the same

wording as Article 8 of the European Convention on Human Rights, which also applies to the UK. It does not seem unlikely that the government will have to contend with the same data protection and privacy rights arguments of its citizens who object to the current access modalties regarding the PSC register. The UK actually does not limit access to the PSC register, it is available to the public free of charge, via the Companies House website. The extent to which the UK nevertheless wants to stick to its current practice and act will possibly also have to be examined from the point of view of competition policy as e. g. investors could critically assess a deviation from the EU standards (Randall, 2023), which ensure stronger protection of their privacy.

#### 2.6.2.2 Financial Court Duesseldorf - FCD (Germany)

The judgment of the Court of 1 June 2011 (FCD, 2011) is a concise example of the principle of „prohibition with reservation of permission“ (in German: „Verbot mit Erlaubnisvorbehalt“ (Frenzel, 2018; Buchner, 2018), which was mentioned above with reference to Article 6 GDPR and which governs all data protection law. Only if the legal provisions for permission applicable to a particular processing of personal data are clearly identified and their statutory facts are given, the processing may be carried out.

The EC/EU-regulations listed under 12.1 prohibit enterprises – in the present context: especially financial services providers – from making funds or other economic resources directly or indirectly available to the persons, companies and organisations listed there in the annexes. The institutions are responsible and must ensure in an appropriate manner that these prohibitions are observed.

The so-called sanctions or embargo lists are updated on an ongoing basis (Däubler, 2021; BAFA, 2009), so that it is expedient to check not only once – such as when establishing a business relationship with a client or at the conclusion of an employment contract – whether the name of the person in question is in the lists. In order to protect themselves from the negative consequences of a violation of the prohibitions the obligated companies also regularly carry out automated checks of the data of all existing clients and employees against the lists (Gola, 2019; Däubler, 2021). This computer-based screening is not required by the regulations themselves: „However, there is no legal obligation to compare the personal data of the employees with the terror lists without any reason in any of these regulations“ (Eder, 2016). Rather, it is a practical and proven instrument for checking identities (Gola and Wronka, 2018).

The Financial Court Düsseldorf therefore stated in its reasons for judgment that the admissibility of this kind of data matching (processing) under data protection law cannot be derived directly from the regulations, but that another legal basis must be used. It referred so far to the „general“ German Data Protection Act (in the version applicable at the time), which essentially provided for the same criteria for permission as were later included in Art. 6 para 1 EU GDPR and UK GDPR accordingly. The literature has followed this finding in principle (Byers, 2016; Eder, 2016; Gola, 2019), although it has given rise to critical comments in the result: While the court affirmed the basic data protection admissibility conditions of ‚necessity‘ and ‚proportionality’ of the comprehensive screening, i. e. including unsuspicious employees, the affirmation of these criteria was repeatedly called into doubt (Ruppert, 2012; Kirsch, 2012; Homburg, 2013).

#### 2.6.2.3 FATF report

The relationship between AML and data protection is presented very comprehensively and transparently in the FATF 68-page report „Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing“ of August 2022 (FATF, 2022c). Right at the beginning (see paragraph 7), the equivalence of the different legal interests to be protected is expressed succinctly as follows: „Detecting, investigating, and prosecuting individuals for ML/TF while protecting individuals‘ data and privacy is not optional; it is essential that both are achieved.“

The report , which contains a plea and encouragement for the exchange of information among financial institutions in the private sector, examines various aspects of the possibilities and already practised procedures of cooperation. It describes the areas and objectives that are of particular relevance for the mutual provision of knowledge between financial institutions (see paragraph 15 Box 2.1). These include inter alia (a) customer identification/verification (for example, whether a customer has previously raised flags or concerns), (b) transaction monitoring (for example, whether abnormal or suspicious activities had been detected), (c) customer screening (for example against domestic sanctions lists) or (d) the identification of the beneficial owner (for example in order to detect shell companies).

In addition to a couple of case studies, to which legal analyses are assigned, further space is given to the description of the data protection framework conditions, some of which differ from country to country, and which limit the flow of information to different extent.

A catalogue of recommendations is intended to support the states respectively the institutions operating there in the development of improved information mechanisms. Although these recommendations are not legally binding – as is the case with all FATF recommendations - they usually are regarded „quasi mandatory“ and do in fact influence the conduct of the addressees.

### 2.7 Complementary regulatory issues: criminal sanctions, administrative fines

A regulator must pay particular attention to the design of penal provisions intended to punish serious violations of statutory prohibitions and restrictions. *“Nullum crimen, nulla poena sine lege”* (engl. “no crime, no punishment without law”) are legal principles not only traditional on the Continent but also enshrined in English law. With the Human Rights Act 1998, which came into force in 2000, the UK adopted Article 7 (1) of the European Convention on Human Rights in identical wording into national law. Even if this “Principle of Legality” requires a clear description of the wrongdoing to be punished as a criminal offense, the problem with the cyber-enabled ML standard is probably less with the legislator and more with its application. The law can limit itself to criminalising ML as such but must not go into all the details, i.e. the modalities of action or methods of practice, used in a ML-process. A judge, on the other hand must grasp and evaluate the technologically enabled *modus operandi* and the inventiveness of a criminal money launderer, and in this way be able to appropriately consider in sentencing the “criminal energy” the lawbreaker has expended. In other words, he must have the technological background knowledge or obtain it – costly and time-consuming – through outside experts in order to be able to pass a fair sentence in a timely manner. This aspect, however, should be subject to further investigation.

These considerations apply according to the punishment of administrative offences, which is the responsibility of the administrative authorities.

Technical expertise is, of course, also a prerequisite for efficient investigative work by law enforcement agencies. A conviction can only be considered if criminal acts can be detected and proven. It is therefore essential to provide the investigating authorities – primarily police and public prosecutors – with the special technical tools they need and to have them trained by cyber specialists. Considering the constantly changing forms of the use of technological practices in ML and the inventiveness of criminals, high demands should be placed on the development of resilient standards in this regard.

## 2.8 Conclusion

The regulatory fight against ML and FT is multi-faced. It begins with the more formal legal question of the regulatory level at which it can be successfully achieved. Basically, two options are available for this. On the one hand, the state can enact laws and enforce compliance with them by means that are also defined by law. On the other hand, the parties concerned, for example the financial institutions and their associations, can agree on appropriate ways and means by way of voluntary private self-regulation.

Almost regularly, the application of the rules involves the processing of personal or individual-related data of those involved in financial transactions. Their right to privacy often collides with the opposing interests of the state and business in prevention and prosecution of criminal behaviour. In this context, data protection law is of particular importance. National and

European legislation, jurisdiction and legally non-binding but de facto mandatory agreements must be observed.

# CHAPTER THREE

# SCHOLARLY ANALYSIS OF MONEY LAUNDERING

## 3.1 Introduction

This Chapter deals with ML from a theoretical perspective. It explains the change in ML techniques from the “analogue” to the digital world. Furthermore, this chapter discusses the possibilities of ML prevention through the use of modern technologies. The analysis is mainly based on a review of current literature. It first covers the topic of ML in general. In this context, the three phases of ML, placement, layering and integration, are described and the relevant literature is reviewed. In the following, the constantly developing technologies are discussed. In particular, the benefits, but also the risks and requirements to cope with these risks are discussed. Finally, this chapter presents the scholarly views on the "new" ways of committing crimes - by using digital technology - from different perspectives, especially those of the supervisory authorities, the law enforcement authorities and the FIs.

The pursuit of financial gain is a primary motivator for those who engage in criminal behaviour (Canhoto, 2021a). Money is the core motivator for both the planning and carrying out of illegal activities (Varga, Brynielsson and Franke, 2021). Around the course of the last three decades, governments all over the globe have shown a rising level of concern over financial crime (Donfouet, Jeanty and Malin, 2018). This concern is spurred by a wide range of issues due to the fact that the effect of illegal financial activity, or simply financial crime, varies widely based on the context (Madsbjerg, 2017). Today, scholars, experts, practitioners and the general lay public generally acknowledge that the existence of economically motivated crime poses a

significant risk to the growth and stability of both the developed and emerging economies (Ariyaluran Habeeb et al., 2019; Henrique, Sobreiro and Kimura, 2019; Albayati, Kim and Rho, 2020). Recognising the impact of crime on national and global development, the United Nations General Assembly (UNGA) adopted the 2030 Agenda for Sustainable Development in 2015 that outlines an ambitious agenda to combat crime (UNGA, 2019). Particularly, in Sustainable Development Goal (SDG) 16, State members of the United Nations set out a range of targets aimed at reducing criminal activity around the world, such as significantly reducing all forms of ML and cyber-enabled financial crimes (UNODC, 2019).

## 3.2 Money laundering and Terrorist financing

### 3.2.1 Money laundering: Characterizations and formats

ML is a prominent type of financial crime referring to the illicit practice of making significant sums of money obtained via illegal conduct, such as drug trafficking or the sponsorship of terrorist organisations, seem to have originated from a legitimate source (Isa et al., 2015; Ryder, 2011; Rocha-Salazar, Segovia-Vargas and Camacho-Miñano, 2021). Criminals of all sorts, from high-level white collar to low-level street gangs, engage in the severe financial offense of ML (Canhoto, 2021b). AML rules may be found in place at the majority of today's FIs to identify and prevent this kind of conduct (Rocha-Salazar, Segovia-Vargas and Camacho-Miñano, 2021). Because the money obtained via the illegal activity is thought to be “dirty”, criminals use a wide variety of ML techniques to make funds appear “clean” (Chau and Nemcsik, 2020, pp.45–49). One method, for example, is the deposit of small amounts of money below the regulatory reporting thresholds into several bank accounts in order to disguise the amount of the transaction – so called “smurfing” (Ryder, 2011). ML is essential for criminal organisations that

wish to use illegally obtained money effectively (May and Bhardwa, 2017). Transactions involving significant sums of unlawful cash are both wasteful and hazardous. Criminals require a method for depositing the money in legal FIs, but in order to do so, they must first provide the appearance that the money originated from legitimate sources (Sciurba, 2019; Song et al., 2019).

Generally speaking, there are three stages of ML: placement, layering, and integration (Ryder, 2011; Sadiq et al., 2019). Through the process of placement, criminal clandestinely transfer "dirty" money into the legal monetary system (Chau and Nemcsik, 2020, p.39). Offender may also conceal the origin of the funds through layering, which consists of a sequence of transactions and creative accounting practices (Macak et al., 2022). The last phase in ML is called integration, and it involves taking the money that has been cleaned out of the legal account so that it may be utilised for whatever the offenders have planned for it (Higney, Hanley and Moro, 2022).

While most illegally generated funds are laundered through the three phases, this model seams insufficient for investigation, understanding, and combating laundering crimes in the contemporary world. By focusing exclusively on the method of ML, the model restricts the scope of counteractive legislation and the investigators' understanding to a negligible component of the crime. Exclusive know-how of the methods of ML is insufficient to fight this criminal activity because it does not answer the most important questions to unravel the entire crime (Cassella, 2018). Investigators should direct attention to establishing the actors behind the crime and their motivating factors. The "who" and "why" questions are critical components for a robust blueprint of AML statutes and efforts. The traditional three-step model is

insufficient since it does not answer these questions. For instance, the model does not identify the authorized actor, such as a banking institution, who facilitates the movement of the laundered money into the global financial system.

On the other hand, the placement, layering, and integration model may expose the sophisticated series of transactions in ML, but this information is mostly irrelevant for prosecution. For instance, information about the means of ML cannot be used in jurisprudence to prove that the money is illegally generated and that the defendant was sufficiently aware of illegality yet proceeded to induce the money into the main stream of commerce (Gilmour, 2023). This shortcoming compromises the utility of the three-phase model in the critical context of prosecution, where the prosecutor has to provide circumstantial evidence to prove the criminality of the alleged act and the defendant's culpability.

The evolution of the technological, regulatory, and business environments may well be the greatest challenge to the utility of the traditional ML model. In their seminal assessment of the motivating factors for ML, Tiwari et al. (2023) revealed that money launderers make multiple considerations before choosing the appropriate strategy to implement the crime.

The scholars explain that multiple interrelated factors, including the actors involved, the predicate crime, the purpose of the crime, and technological innovations determine why and how money launderers move funds into the economy. Most importantly, the traditional model of tracing fails entirely when subjected to the current context of laundering through investments in crypto assets. These investments use blockchain technology involving transaction records in multiple places simultaneously such that it is impossible to identify the person actors(s) behind any independently occurring activity (Thommandru and Chakka, 2023).

Blockchain technology can facilitate ML through enhanced autonomy and obfuscation of the path through which money penetrates into the economy.

The traditional placement, layering, and integration model is inadequate for navigating the network formed by the interaction of these motivating factors and should be complemented or substituted with a holistic approach to understanding the comprehensive elements of ML. The illegality of the proceeds and the culpability of involved actors are fundamental elements that must be uncovered to fight contemporary ML.

### 3.2.2 Relationship between Money Laundering and Terrorist Financing

ML plays an important role in regard to FT. It may involve funds obtained from legitimate sources such as personal donations and profits from businesses and charitable organisations (Canhoto, 2021b). Therefore, FT is often referred to "reverse" ML (Krieger and Meierrieks, 2011). Additionally, it may involve funds obtained from illegal sources such as the trafficking of drugs, fraud, smuggling, kidnapping, and extortion (García-Retuerta et al., 2019). It involves the provision of finances or funding to individual terrorists or non-state actors with the intent to mete out violence and intimidation against innocent civilians to achieve a political aim.

Terrorism is the planned and purposeful use or threat of use of extreme violence or cruelty by sub-national organisations to attain a political, religious, or ideological aim through public intimidation, even though the targeted public is not directly involved in making policies and decisions the terrorists demand to influence (Canhoto, 2021b; Rocha-Salazar, Segovia-Vargas and Camacho-Miñano, 2021). Financing is necessary for terrorist organisations in order to sustain its logistical hubs, attract and recruit new members, and carry out operations (Masciandaro, 2017; García-Retuerta et al., 2019). To move their finances, terrorist

organisations use the official banking system, informal value-transfer and agent-based transfer channels, and the actual transit of cash, gold, and other valuables through smuggling routes.

### 3.3 Emerging technologies – Benefits, risks and requirements

There is no question that the ongoing growth of digital technologies, the rise of fintech companies, and a rising dependence on cryptocurrencies and other alternative means of payment offer businesses with opportunities that have never been seen before (Barroso and Laborda, 2022). On the other hand, they mark the beginning of a new age of financial crime, one that is characterised by intricate interconnection and ambiguous geographies. It should come as no surprise that global authorities are having trouble keeping up with the constantly evolving environment (Priebe and Markus, 2015; Barroso and Laborda, 2022; Macak et al., 2022).

Diverse reasons, such as automation and digitization's inherent susceptibilities to financial crime, the explosive development of transaction volumes, and the increased internationalisation of financial systems, pose risks for banks (Beer and Burrows, 2013; Hanafizadeh and Marjaie, 2021; Barroso and Laborda, 2022). Additionally, cybercrime and harmful hacking have increased. In the realm of financial crime, authorities are constantly revising the regulations to account for unlawful trafficking and ML, and governments have intensified their use of economic penalties against nations, public and private businesses, and even individuals (Wessels et al., 2021; World Bank, 2022). Institutions are discovering that their current ways of combating such crimes are inadequate to meet the many dangers and burdens (Madsbjerg, 2017). For this reason, executives are modernising their operational models to acquire a comprehensive perspective of the ever-changing financial crime scenario. This

perspective serves as the foundation for efficient and successful fraud risk management (Al-Hashedi and Magalingam, 2021).

Taking into account factors such as the pseudo-anonymity of blockchain transactions, the lack of clearly defined regulatory regimes, and the challenges faced by law enforcement in attempting to seize illegal proceeds that are in the form of cryptocurrencies, the potential for ML and the FT organisations becomes abundantly clear (Deloitte, 2022). Many regulators obligate FIs to give greater thought to the risks presented by emerging technologies, such as e-wallets, cryptocurrencies, prepaid cards, and applications that allow for private money transactions using mobile services, in order to address these concerns (Azinge-Egbiri, 2021; 2021). FIs need to modify their risk-based approach so that it takes into account the implications of ML and FT that are raised by new technologies and new ways of conducting business if they want to keep up with the rapid evolution of technological innovation (Masciandaro, 2017; Cheng et al., 2021). This may be as easy as asking what risks and opportunities are posed by these technologies, as well as what safeguards and precautions they can take to protect against such threats and vulnerabilities (Abreu, Kimura and Sobreiro, 2019).

In view of these facts, compliance professionals working in the financial crimes arena need to immediately begin acting in accordance with the obligation to innovate (Thompson, 2017; Paschen, Pitt and Kietzmann, 2020). For example, much of the time spent by investigators of suspicious conduct is now consumed with the search for information and the collection of documents (Cheng et al., 2021). Investigators will be able to devote more of their time to managing risks if the aforementioned duties are automated, for example via the use of robotic process automation (RPA) (Zhang and Trubey, 2018). In a similar vein, firms might automatically

resolve false alarms without human intervention if they used sophisticated analytics to monitoring financial transactions (FATF, 2018b). This would free up analysts to focus on higher-level threats. Notably, this sort of automated solution does not even come close to exploring the full scope of what is conceivable (Abreu, Kimura and Sobreiro, 2019). Even though most businesses are quite good at collecting data, they have a hard time converting that data into insightful information that can be used to guide business choices and decisions (Albayati, Kim and Rho, 2020). The world is moving towards a period of time known as hyper-personalisation, which is characterised by the fact that technology may be utilised to comprehend the actions and reasons behind individual customer behaviour (Balani, 2019). The use of this sort of model to identify illegal behaviour or improve know-your-customer (KYC) initiatives has the potential to completely transform AML compliance (Albayati, Kim and Rho, 2020). Compliance professionals can do more than just work faster when they have this kind of technology at their disposal. They can also improve their capacity to combat and actually prevent financial crime as a group (Deloitte, 2022).

### 3.4 Fighting financial crime enabled by digital technology

The global community has prioritised the fight against financial crime, paying special attention to ML and FT, due to the effects that these specific types of crime have on the economy, government, and society (Rider, 2015). The global community, including governments and other organisations, is worried about financial crime (cf. INTERPOL, 2021, for example). As one of the aims of this effort is to maintain the efficiency, transparency and security of the global financial system, cutting off terrorists' access to financial resources accessible, and making it harder for criminals and fraudsters to benefit from their illegal actions (Deloitte, 2022). But

more cooperation between the various regulatory organisations and institutions is necessary for both the public and commercial sectors to regulate and evaluate financial crime.

Because money plays such a key role in enabling and inspiring illegal conduct (Sciurba, 2019), actions that delay the movement of money in a criminal transaction are critical in the global fight against financial crime (Isa et al., 2015). Businesses in the financial sector play a crucial role in facilitating the free circulation of money across the world (Azinge-Egbiri, 2021). Records are generated when money moves through the financial system, and they may be used to learn more about the circulation, creation, and use of currency (Canhoto, 2021b). In an effort to curb criminal activity, governments throughout the globe have enacted regulations obliging financial service providers to examine customer behaviour (FATF, 2022c). To fulfil this requirement, financial service providers should consider factors such as a customer's background, occupation, source of income and wealth, country of origin and residence, products used, nature and purpose of accounts and business activities (Basel Committee on Banking Supervision, 2016).

AML and CFT regimes in FIs and government are, perhaps, the most applied and major mechanisms employed to fight financial crime in the digital age. AML refers to a collection of regulations, protocols, and technology that work together to stop the laundering of money (Chau and Nemcsik, 2020). It is used to detect possibly fraudulent activities and is applied into government systems as well as the systems of big financial institutions (Sullivan, 2015). FIs are subject to stringent requirements on the implementation of processes to detect financial crimes. They are required to spot, monitor, act on and report suspicious customer activity (Balani, 2019). Additionally, they should have divisions devoted to tracking criminal

and fraudulent transactions (Singh and Best, 2019). CFT refers to a collection of laws, rules, and other procedures implemented by the government with the purpose of limiting access to money and financial services for individuals and organisations that the government deems to be terrorists (García-Retuerta et al., 2019; Azinge-Egbiri, 2021). If law enforcement is able to track and trace out the origin or sources of the finances that are used to support terrorists in implementing activities related to terrorism, there is a chance that mandated institutions will be able to stop all or at least part of those acts from being perpetrated (Ashok et al., 2021). CFT is often closely tied to AML. When law enforcement agencies are able to identify and stop operations that involve ML, they may also be able to stop those resources from being used to support acts of terrorism (García-Retuerta et al., 2019; Canhoto, 2021b; Rocha-Salazar, Segovia-Vargas and Camacho-Miñano, 2021). The fight against ML is an essential component of CFT (Whisker and Lokanan, 2019). Instead of attempting to apprehend a criminal who is planning or carrying out an act of terrorism through some other methods, law enforcement agencies may address the issue from the financial side of things by tracking the flow of financing that supports the operations (Singh and Best, 2019; Azinge-Egbiri, 2021; Tertychnyi et al., 2022).

A significant number of institutions have implemented a policy known as KYC which is designed to assist in identifying and flagging potentially fraudulent transactions based on individual customers (Masciandaro and Filotto, 2001). The KYC process usually divides into two subprocesses aknowleging different levels of aml risks with regards to the customers. Those are called customer due diligence (CDD) and enhanced due diligence (EDD). FIs keep meticulous records of their transactions and operations in order to provide law enforcement with the

information necessary to track down the origin of criminal activity (Varga, Brynielsson and Franke, 2021; Deloitte, 2022; ICA, 2022).

Controls are also put in place by a variety of organisations, including enterprises, governments, and financial institutions, to combat ML (Sciurba, 2019). The first of them is that the government has made it a crime (Whisker and Lokanan, 2019). Guidelines that enable countries to bring criminal charges against persons participating in ML schemes have been outlined in the United Nations Convention Against Transnational Organized Crime (Vandezande, 2017; FATF, 2022b). Institutions like the FATF also exist to ensure that international AML standards are put in place to prevent financial crimes (Arslanian and Fischer, 2019). Even though businesses of this kind are required by law to comply with AMLrules specific to the jurisdiction in which they are based, there is no guarantee that they will do so (May and Bhardwa, 2017). The procedures for putting the policies into practice are sometimes expensive and fruitless, calling into question the overall value that may be derived from having them in place (Azinge-Egbiri, 2021).

The majority of FIs demand that deposits be held in an account for a certain amount of time, usually five days (Burnes et al., 2017; Ho, Ko and Mazerolle, 2022). This holding time helps control the risk that is connected with money moving through banks for the purpose of ML (Masciandaro, 2017; Brands and Van Doorn, 2022). Businesses and FIs alike use transaction-tracking software and retain complete records of all financial dealings (Deloitte, 2022). Information about customers may be sorted into categories according to their perceived risk, and transactions may be declined if customers' conduct or transactions fall within the risk behaviour or conditions that require transactions to be declined. This also helps in the procedures of anomaly detection (ICA, 2022).

Domestic government agencies, international regulators and supervisors as well as institutions operating in the financial sector are increasingly focusing on cybersecurity and cyber risk due to the growing danger and effect of cyberattacks on the financial sector. According to published figures, users of the financial services sector were subjected to a staggering 65 percent more cyberattacks in 2016 than users of any other sector or industry (Barboza et al., 2016). This figure represents a 29 percent rise from the previous year. Cyberspace attacks are becoming more sophisticated, frequent, and persistent, and cyber threats are becoming more severe and complex, risking disrupting the linked global financial systems and the institutions that manage and support those systems (Ahmed, Deokar and Lee, 2021; Al-Hashedi and Magalingam, 2021). Similarly, cyber risk is posing an increasing and severe danger to the integrity and efficiency of the financial sector throughout the globe. To make matters worse, the inevitable tendency towards entirely digital client contacts exposes the banking industry to cyber dangers (Dibrova, 2016; Vandezande, 2017). In this environment, about more than half of all bank customers are already exclusively digital. Furthermore, the number of clients who communicate physically with bank employees is decreasing. For example, HSBC announced recently that it will close 114 branches of the bank in the UK from April 2023 onwards (White, 2022).

It is critical to improve cooperation and coordination between financial sector regulators and supervisors and other entities engaged in cyber risk and cybersecurity matters. In relation to fighting cyber-enabled or cyber-related financial crime, organisations are increasingly adopting novel and innovative digital technologies and techniques to help in the identification of anomalies in digital company finance systems (Manuela and Ricardo, 2020). For instance, digital forensics, or the use of informatics to preserve the integrity of digital crime evidence material

and maintain a strict chain of custody, may be an important tool in the fight against cyber-enabled and related financial crime (Sadiq et al., 2019). In the end, digital forensics is all about collecting evidence that may help figure out the what, who, when, where, why, and how of a financial crime incident (Ain et al., 2019; Brands and Van Doorn, 2022). Depending on the answers given, the claims made about a digital monetary criminal activity are explored and examined (Macak et al., 2022).

Several of the world's developed and developing jurisdictions are increasingly taking steps to improve their regulatory and supervisory systems in order to combat cyber risk and enhance cybersecurity in their financial sectors (Ibrahim, 2016). One of the steps include establishing multi- and inter-agency cyber-risk coordination, regulatory and supervisory protocols analogous to those in place for financial stability (Holt and Lavorgna, 2021). Another shared best practice suggests the need for participants in the domestic and global financial sectors to share cyber-related data and information that is voluntarily, if not mandatorily, and anonymously exchanged among them. Third, in some countries, FIs are required to create an information and communications technology (ICT) strategy and risk management framework (Ho, Ko and Mazerolle, 2022). This must include incident response plans that have a clear chain of command so that appropriate business choices can be made (Brands and Van Doorn, 2022). Additionally, the employment of a designated information security officer is necessary in several nations. Lastly, in some countries, employees at FIs are required to routinely put their incident response abilities to the test through testing and simulations (Deloitte, 2022).

However, the ever-changing digital landscape demands constant changing of policy and strategy (Masciandaro and Filotto, 2001). Because cybercrime is evidently an ever-present

threat, governments and regulatory agencies have been obliged to place a greater emphasis on AML/CFT concerns (Vandezande, 2017). For instance, because cybercriminals are developing malware, digital applications and other mechanisms to exploit either natural or synthetic data, the incidence of identity-based fraud has increased (Whisker and Lokanan, 2019). It is becoming increasingly untenable to take a siloed approach to the largely interconnected cybersecurity risks; it is abundantly evident that the operational paradigm has to be rethought (Sciurba, 2019).

AML/CFT systems are required to be pomwerful, but they also have to satisfy additional criteria, such as high standards for data security, confidentiality and client privacy, in addition to demands for identity verification (Zimiles and Mueller, 2019). In addition, according to domestic and international law, institutions that provide financial services are required to be able to demonstrate at all times that the technologies they use do not unjustly prejudice against any of their clients (Sullivan, 2015). Because of these requirements, FIs are often apprehensive about adopting technologies in which they do not have full control over, particularly in regard to the use of customer data; or whose installations they do not fully understand (Singh and Best, 2019). The AML/CFT technology that is used to detect anomalies and suspicious behaviour that is tied to financial crimes, cyber risk and the regulation and supervision of the financial sector to curb ML and FT is always evolving as it gears up towards more accuracy (Tertychnyi et al., 2022). These systems are able to advance in sophistication with the help of technologies such as AI, regulatory technologies, and Big Data software designed for analysing large amounts of data. However, such systems are often seen as black-box type of algorithms and machine learning models where institutions only understand inputs

and outputs but have no knowledge of its internal working (Bell, 2002). In other words, while AML/CFT systems seem useful and ready for machine learning deployment, and several players in the financial sector have invested in the AML/CFT technology, a number of organisational and technical barriers still largely exist that call for attention (Sullivan, 2015).

## 3.5 Conclusion

The analysis of the relevant literature has shown that ML also plays a major role in the scholarly debate. There are different views on the reasons for the development of ML discussed, including the validity of the three phases of ML.

However, the literature is not limited to presenting a multitude of facets of the problem area of unlawful cyber-enabled ML, which has taken on a constantly growing scale due to the rapid development of ever new technological instruments and practices for committing offences. At the same time, the authors describe a broad spectrum of the methods already in use to combat the offences, which is supplemented by numerous suggestions for further measures.

It is clear from the analysis of the literature that effective combating and damage defence cannot be carried out or achieved by the state alone, i.e. its legislation, jurisdiction or administration. In this respect, reference is made to an extensive scenario of corresponding initiaves and strategies that have been and continue to be developed by the private sector, e.g. by financial service providers. The following chapter 4 takes up this area of private control and combating cyber-based financial crime under the aspect of regulatory action.

# CHAPTER FOUR

FINDINGS, RECOMMENDATIONS AND CONCLUSION

## 4.1 Focal legal issues

Two topics appear to be of particular importance in the context of the present study. One refers to the relationship between state law and self-regulation and concerns the question of which regulatory regime can successfully achieve the fight against ML and FT, the other how the protection of the privacy of those involved in financial transactions is designed, i.e. the data protection aspect.

The fact that both regulatory systems – state intervention and self-regulation – are applied can be seen in a number of examples. Whether one should be given priority over the other is occasionally discussed (Ofcom, 2008; Wahlers, 2011; Wronka, 2020), but is ultimately an academic question. Both concepts, whose significance is largely determined by the respective national legal culture (cf. UK vs. continental law), have their advantages and disadvantages (Wronka, 2020). What is decisive is their efficiency. Moreover, state and private rules are not always sharply demarcated from each other. This applies not only to so-called "co-regulation" (Ofcom, 2008), but also in cases where administrative action is influenced by the content of private guidelines. In this respect, there is an interaction between self-disciplinary and state regulation.

### 4.1.1 Self-regulation

The term "self-regulation" covers rules with different names and sometimes very different approaches. Common headings are "code of practice", "code of ethics", "code of conduct",

"code of behaviour", "standards for best practice" or simply "best practices" (Castro, 2011; Wronka, 2020). A few examples are intended to illustrate this against the background of the UK-specific regulatory regime.

#### 4.1.1.1 Financial Conduct Authority (FCA)

The heading "Code of Conduct" above a set of rules does not necessarily mean that it is a self-regulatory code in the sense outlined above. In the present context self-regulation "concerns groups of firms in particular industry or entire industry sectors that agree to act in prescribed ways, according to a set of rules or principles" (OECD, 2015). For this reason, the FCA's "Code of Conduct" (COCON, FCA handbook) is not to be compared with the regime of rules defined by the private sector to which the participating firms and institutions voluntarily submit. Rather it is the execution of a statutory mandate resp. the exercise of a statutory authorisation - stipulated in section 64A of the Financial Services and Markets Act - by an authority, i. e. a state institution.

Most of the rules compiled in COCON 2.1 and COCON 2.2 are not very specific but rather basic postulates for decent and fair business conduct in any industry sector. They are relatively general and, with a few exeptions, self-evident. For example, COCON 2.1 states: "You must act with integrity" (rule 1), "You must act with due skill, care and diligence" (rule 2) , "You must pay due regard to the interests of customers and treat them fairly" (rule 4), "You must observe proper standards of market conduct" (rule 5).

More concretely, precisely and directly related to the area of ML discussed here the general COCON requirements affect also the "Systems and Controls" Sourcebook, which is also a part of

the FCA handbook. In the section "Systems and controls in relation to compliance, financial crime and money laundering" (SYSC 3.2.6) numerous instructions and obligations are formulated, especially for senior managers and executive boards. They are listed in some detail, but a distinction is made between "must" and "should". In general, the establishment of comprehensive and adequate operational systems and controls to combat ML is mandatory (SYSC 3.2.6A), while only indications are given regarding the criteria to be taken into account when identifying risks in this regard; a series of factors is enumerated for clarification in SYSC 3.2.6F.

An important statement concerning self-regulatory approaches and their significance for the FCA's assessment practice is to be found in SYSC 3.2.6E: "The FCA, when considering whether a breach of its rules on systems and controls against ML has occured, will have regard to whether a firm has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group". This view is to be returned to at 2.5.1.3.

#### 4.1.1.2 CryptoUK

Both the COCON rules and the SYSC-requirements radiate to the codification of private guiding principles. An example of this is the CryptoUK "Code of Conduct" (CryptoUK, 2018). The CryptoUK is a self-regulatory trade association founded in 2018 in the cryptoasset sector, which has set itself the goal to improve higher standards of conduct (see homepage). The Code, to which the members have subscribed, consists of a catalogue of a total of 10 declarations of commitment. These include, for example, obligations, aligned with the FCA Code, to operate honestly and responsibly in their relationships with consumers or to provide communications

(inter alia marketing and promotional material) with customers that are fair, clear and not misleading.

In the majority, however, detailed sector-specific rules are established. They concern security aspects, the obligation to cooperate with the authorities in the event of discovered illegal activities by customers, the performance of due diligence checks on platform users to prevent illegal activities such as the financing of terrorism, halting trading in case suspicious activity is identified and closing any accounts engaging in such activity etc.

The ten "commandments" represent principles, but do not contain practical recommendations, such as which technical tools and techniques could be used for the "security architecture" or for client screening, or which concrete organisational measures should be taken.

#### 4.1.1.3 Joint Money Laundering Steering Group (JMLSG)

The JMLSG is a private organization whose members are currently 14 UK associations in the financial services industry (JMLSG, 2023a). Its primary mission is to provide assistance to members in complying with the legal requirements placed on them to combat and prevent ML and terrorist financing. The comprehensive 3-part compendium, titled "Guidance For The Financial Sector," is not legally binding, although it is approved by the Uk Treasury.

In terms of content, it consists of a mixture of commentary-like explanations of statutory provisions and administrative requirements (FCA), supplemented by advice and recommendations on the design of operational measures. However, it is emphasized that the "Guidance" should only form a basis for company-specific arrangements ("tailored policies and procedures that are appropriate for their business", "... allows them some discretion as to how

they apply the requirements of the UK AML/CFT regime in the particular circumstances of the firm...").

However, if firms wish to deviate substantially from the "Guidance", they must document this and, if necessary, justify it to the FCA (JMLSG, Preface, paragraph 29).

The generally applicable basic statements relating to the entire financial sector can be found in Part 1 of the Guidance, while Parts 2 and 3 deal with sector-specific issues. For example, some of the 8 chapters in Part 1 deal with management accountability, internal controls, customer due diligence, customer risk assessments, suspicious activities, staff training and awareness, and record keeping. The issues associated with these key points and the resulting obligations to act are presented in detail.

In Part 2, a recently adopted and here particularly interesting amendment is to be highlighted, which relates to cryptoassets transfers and provides interpretations, explanations, etc. concerning regulations 74 A-C of the Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 - the so-called 'Travel Rule' (JMLSG, 2023b). They apply to crypto exchange providers and custodian wallet providers and, in short, relate to their obligation to provide specific information on the sending owner of the crytoasset resp. the initiator as well as the intended recipient of the cryptoasset, the measures to be taken and decisions to be made by them in the absence or ambiguity of this information as well as the required risk management approach. This brief description of the content of the "Guidance" should end with some comments:

Like the CryptoUK "Code of Conduct", the JMLSG "Guidance" does not contain any detailed, precise "instructions for use", e.g. with regard to the use of specific tools and technology or how, with what effort and to what extent the various risk controls are to be carried out. However, this omission can be explained. On the one hand, the "Guidance" is only intended to clarify the obligations of the firms and to provide an orientation, a basis for the firm-specific implementation measures to be initiated. The Guidance is therefore not to be understood as exhaustive and is deliberately intended to provide scope for practical implementation and supplementation.

On the other hand, the JMLSG is an organization of heterogeneous member associations, an umbrella federation, so to speak. The possibilities and needs of the firms that are members of, for example, the Association of British Insurers and the Building Societies Association are naturally different. Standardization of practices would not be appropriate.

However, it also follows that the member associations are not prevented from further tailoring the guidelines for action to their member companies. They are at liberty, within the framework of their legal possibilities, to make corresponding recommendations.

### 4.1.2 Legal Limits to self-regulation

There is consus that industry self-regulation is based on the principles of private autonomy. This means that individual firms and the organizations representing their interests are basically free to determine in which way they want to regulate matters, i.e., which rules should apply to their market behavior and thus to competition. Likewise, it is not controversial that the exercise of private autonomy is limited. There are certain areas of social life that require state order and state intervention, including coercive measures if necessary, to safeguard them, while others do

not (cf. 2.4 and 2.7). It is indisputable, too, that self-regulatory rules may not contravene constitutional or other statutory provisions or supreme court decisions, for example (Wronka, 2020). In the present context, the question of whether and, if so, in which areas self-disciplinary rules inadmissibly influence competition, i.e., come into conflict with state competition law and antitrust law, could become particularly important in this respect. The OECD report (OECD, 2015) addresses this aspect as follows: "Self-regulatory arrangements can be used to develop and maintain common standards, providing level playing fields that facilitate the entry of newcomers and promote competition. On the other hand, those arrangements which favor incumbents, while beneficial to those concerned, can act to limit competition" (p. 11).

The JMLSG avoids this potential conflict by distinguishing in its self-regulatory "Guidance" - as is also done in the SYSC of the FCA - between directly binding, mandatory provisions and those that only provide guidance on certain measures. The former are identified with the term "must", the latter with the term "should": "...the guidance uses the term "should" to indicate ways in which the statutory and regulatory requirements may be satisfied, but allowing for alternative means of meeting the requirements" (Preface, paragraph 19).

From this, the following observations can be made: A self-regulatory set of rules such as a "code of conduct" or a catalog of "best practices" or "guidelines" etc. must not be judged as a whole according to whether it possibly violates state law; the decisive factor is rather the individual contents of the rules. If they - or some of them - are not mandatorily prescribed by an association, but rather formulated as suggestions, or if alternatives to be freely chosen are listed as examples, it is not recognizable that the association or its members are behaving in an anti-competitive manner. Moreover, if the autonomously established rules were to receive

state approval, as it is the case with the JMLSG-"Guidance", this would undoubtly be accompanied by an official review of whether particular provisions are incompatible with competition law – an additional safeguard, so to speak.

Despite the existing dense regulatory framework - especially in the UK - it is apparent that important questions for the practice of the financial industry have not been exhaustively answered and should be supplemented (see recommendations below).

### 4.1.3 Data protection

The second point, which was raised at the beginning of this chapter and discussed in more detail in chapter 2, relates to the compatibility of measures to combat ML and FT with the principles of data protection.

Data protection and AML are, as it were, inextricably linked, as examples from jurisdiction, state and private bodies show. In addition to complex presentations of the resulting legal problems, such as those compiled in the FATF document, there are also separate publications on specific issues. For example, the UK Treasury has published a guide - marked as non-binding - on the handling of information requests (HM Treasury, 2002), which is still being supplemented with explanations by the JMLSG.

## 4.2 Practical challenges

There are practical problems associated with the legal issues. They concern both the recognition of acts of abuse, which requires a great deal of technical knowledge and equipment, especially in cyber-enabled transactions, and the necessary expertise and technological and personnel requirements for appropriate defence measures. The first aspect is

not only of great relevance for the FIs directly affected, but also for the state prosecution bodies and the courts. The possibilities and the willingness to provide the necessary financial means to eliminate corresponding deficits play a not insignificant role.

## 4.3 Recommendations

### 4.3.1 Preliminary remarks

It was noted that despite the sometimes very comprehensive descriptions (FATF, FCA, JMLSG) of measures to combat ML and FT, more concrete implementation instructions are lacking or particular aspects are not sufficiently addressed. The explanations of state, in particular legal requirements achieved with these documents and the related advice and recommendations for financial institutions are intended to cover a wide range of users and cannot, by their very nature, offer differentiated solutions. Large FIs, for example, have more and other factual possibilities of implementation, both financially and in terms of staff and logistics, than small firms. Statements on how and to what extent the staff of financial service providers, who also represents a potential danger with regard to possible involvement in illegal transactions, must be controlled also appear insufficient. Some examples are given below.

### 4.3.2 Additions to the regulatory framework

Notwithstanding the legal limits imposed on state legislators for intervening in market behaviour, laws can become intransparent if they are overloaded with minute details. Rather, administrative law can be used to achieve targeted, practice-oriented additions to and explanations of the content of laws - as is done in the UK by the FCA and in Germany by the BaFin (Federal Financial Services Agency). Insofar as national supervisory authorities are not expressly obliged or authorised to do so by law, they can do so in any case within the scope of

their duty of care. However, authorities are often overburdened - they lack time, staff and financial resources, as is the case with BaFin, for example.

It therefore stands to reason that the business sectors concerned take on this task, which is in their own interest, with the means of self-regulation available to them. Which form of presentation is chosen is of marginal importance, as shown above in chapter 2 paragraph 2.5.1.

### 4.3.3 Examples

The need for further assistance for financial service providers can already be seen to some extent in the "Guidance" of the JMLSG.

i. The use of automated screening systems

   The question of whether and by which FIs automated screening processes must or should be carried out is answered only vaguely: "Some firms, for example large firms with millions of customers or which process many millions of transactions every day, will use automated screening systems. Other firms with smaller numbers of customers and transactions may achieve compliance through other processes" (JMLSG-Guidance, part 3, p. 46).

   It should be possible for the trade associations that are members of the JMLSG to define criteria in this regard specifically for their member firms and to make corresponding clear recommendations.

ii. The designation of technical tools (hardware, programs, etc.), including their producers resp. providers, which can be used for screening processes (customers, transactions, employees, etc.).

"Firms may consider whether and what type of screening software to use in line with the nature, size and risk profile of their business" (JMLSG-Guidance, part 3, p. 56).

As mentioned above, there are no legal obstacles for trade associations to present several such programmes, their sources of supply and procurement costs to their member firms and to offer them a choice. Especially smaller companies that are not familiar with the market need guidance.

iii. The frequency of screening processes

"Less immediate or frequent screening and/or being more selective with regard to those who are screened" (JMLSG-Guidance, part 3, p. 46)

The JMLSG is not in a position to provide its heterogeneous member associations with specific criteria for risk assessment. However, this is possible for the trade associations with regard to their members. It should be borne in mind that, for example, very different time periods for inspection frequencies are discussed in the literature with regard to the employees of financial service providers (Gola and Wronka, 2018). If, however, screening is automatically carried out too frequently "as a precaution", such interventions, which foreseeably do not generate any new findings, may meet with data protection concerns (Gola and Wronka, 2018).

iv. Ongoing function control of screening software

"Firms should also monitor the ongoing effectiveness of automated systems...and should perodically check the software is working as they expect it to" (JMLSG-Guidance, part 3, p. 56).

References to "periodicity" are probably unnecessary for large firms, as they will regularly perform checks on the entire IT infrastructure. However, it would help smaller financial services firms if such periods were defined by their associations.

v. The literature points to more aspects that play a major role in the practical operation of risk assessment of clients and transactions, but which are in part too weakly developed (Maume and Maute, 2020) and that are suitable as the subject of self-regulatory approaches, among them

   - the provision of sufficient financial resources for the maintance of hardware

   - the arrangement of hierarchy-related staff training measures

   - the involvement of external experts.

vi. Advice and recommendations to FIs on data protection-compliant behaviour, for example with regard to the storage of suspicious activity indicators, would also be desirable: How long may they be stored if the suspicion is not confirmed? Where should they be stored? Who may have access to this highly sensitive data? What technical and organisational security measures should be taken to prevent unauthorised access?

#### 4.3.4 Strengthening self-regulatory measures by anchoring them in laws

There are a number of national laws that explicitly refer to the existence and content of self-regulatory rules; this is also the case with some European legal acts (Wronka, 2020). The expressed legislative recognition of soft law should also be transferable to the area of cyber-based ML. This approach would have greater significance for European-continental law than for the Anglo-American legal system. A direct anchoring of private conventions of conduct in state

law would decisively increase their importance, at least in the European legal area. A recent example is Article 40 of the EU GDPR, which even mandates the EU member states to promote self-regulatory rules of conduct.

Therefore, the recommendation is made to explicitly give room to cyber-specific self-regulatory systems through legislation in the context of AML and counter-terrorism provisions. In other words: The European and national legislators should expressis verbis encourage the financial sector to develop self-regulatory mechanisms with a specific view to cryptocurrencies in the sense described.

These private rules do not have to detach themselves from state influence; on the contrary, they are strengthened when they are under state observation (Wahlers, 2011). Trade association rules, that serve the understanding and application of state regulations and complement these receive their special quality if they are approved by the State (analogous to Article 40 (5) of the GDPR, for example, and their compliance is monitored by the state (analogous to Article 41). The approval means a kind of quality confirmation or cachet (Weichert in Däubler et al., 2020). For those committed to the rules, it offers legal certainty and competitive advantages over the other competitors by conveying seriousness, reputation (OECD, 2015), reliability and truthworthiness.

### 4.4 Conclusion

The primary concerns to be addressed in ML using cryptocurrencies are anonymity and decentralization, and rules are failing to handle these issues with this currency. Criminals employ cutting-edge technology to exploit firms' vulnerabilities in order to carry out significant crimes. Using only traditional methods to combat cyber-laundering schemes is not sufficient.

Monitoring, detecting, and regulating transaction infractions is nearly challenging for FIs. With digital payment systems becoming the standard in society, fraudsters can now launder money using traditional means because transactions are apparent in milliseconds. To detect and prevent new ML methods, VASPs, which have the relevant competence in the area, must be involved.

The legal issues examined in more detail focus on two areas. On the one hand, there is the question of the regulatory framework within which the fight against ML and FT can be achieved and whether the regulatory content is sufficient for effective counter-measures. On the other hand, there is the question in which way data protection law influences these measures.

On the one hand, the fight against ML and FT can be achieved by state intervention, in particular laws and administrative measures, but on the other hand, it is also possible at the level of private law through self-regulation by the affected industry, i.e. the financial sector.

There are a large number of state regulations at national and European level aimed at combating ML and FT. They are flanked by relevant legislation. There exist also self-regulatory sets of rules and explanations, some of which - especially in the UK - are very extensive. Despite the broad spectrum of regulated issues, there is often a lack of practical, concrete instructions for action. A number of examples illustrate this. It is therefore advocated that appropriate implementations resp. additions be made by means of self-regulatory mechanisms.

As a rule, natural persons are involved in ML-related activities in some way. The FATF has described and evaluated numerous case constellations that are trend-setting for financial transactions worldwide. In addition, state institutions, e.g. the FCA, and organisations of the

financial industry, e.g. the CryptoUK, have developed rules concerning data protection, especially with regard to control measures. Not only these documents, the content of which will be briefly outlined, but also national and EU jurisdiction make it clear that data protection principles set limits to measures intended to combat ML and FT. There is a conflict situation: a balancing of the respective protected legal interests must always be achieved, i.e. between the individual right to privacy and the interest of the state and the general public in the functioning of the financial system.

No less weighty than regulatory gaps seems to be the problem of recognising and assessing cyber-enabled ML abuses and the lack of knowledge of appropriate practices to defend against attacks on the part of obligated parties. Although the legislator can formulate requirements and prohibitions, enforcement is limited by a lack of sufficient understanding of the content of the provisions, a lack of technical or organisational expertise and a lack of willingness to invest in technology and personnel.

Service providers should be encouraged not to cut corners on equipment, programs, training, or personnel at the expense of a comprehensive risk analysis in order to avoid the financial burden. This applies accordingly to the work of law enforcement agencies.

# CHAPTER FIVE

PUBLISHED ARTICLES

## 5.1 Introduction

This chapter contains the text of the pubished articles, furtherance to the objective of this thesis. Summaries of the main features of the articles are outlined in the first part of the chapter. The second part of the chapter contains the original text of the articles.

## 5.2 Summary of the articles

### 5.2.1 Money laundering through cryptocurrencies Analysis of the phenomenon and possible prevention measures

The article 'Money laundering through cryptocurrencies Analysis of the phenomenon and possible prevention measures' provides in-depth information on the ML phenomena. It provides in-depth background on ML, cryptocurrencies, and financial regulations. It also explains the methods and techniques used in ML, the suitability of cryptocurrencies in ML, and why the current regulations are not adequate to counter the vice. A closer analysis of the amending directive to the 4$^{th}$ AMLD reveals that other relevant players in the crypto market, such as mixer and tumbler services, are also not covered, though these actors are most frequently used for ML.

The article recommends therefore to consider the inclusion of providers of such services as obliged parties under ML law in the wording of the sixth Anti-Money Laundering Directive. At the same time, however, regulation should also be careful not to unnecessarily hinder technological diversity or restrict the rights of legal users.

### 5.2.2 “Cyber-Laundering”: The change of money laundering in the digital age

The article ‘"Cyber-Laundering": The change of money laundering in the digital age’ is a qualitative study on how the development in the digital space influences ML. Criminals are leveraging today's technology to orchestrate significant offences, such as cyber laundering, which is not restricted by data protection. It's virtually impossible for banks to track, detect, and punish transactions.

Therefore, the article recommends that banks need to further develop their internal risk measures to prevent the usage of cryptocurrencies for illicit purposes.

### 5.2.3 Anti-Money Laundering Regimes: A comparison between Germany, Switzerland, and the UK with a focus on the crypto business

The article ‘Anti-Money Laundering Regimes: A comparison between Germany, Switzerland, and the UK with a focus on the crypto business' examines the current framework for regulating cryptocurrency in three European countries, Germany, UK, and Switzerland. Overall, findings suggested that the AML laws are additionally modified to include the cryptocurrencies violations of the legislation, as it is the decentralized financial systems generating opportunities for crimes and terror financing. Moderate or mild laws were found in Switzerland following Germany while the UK has the most traditional and stringent laws on ML.

The article recommends that the principal issues with ML and tax evasion through cryptocurrencies need to be addressed in the regulatory framework, especially the “anonymity” around transactions and the issue of decentralization. However, the 5$^{th}$ EU-Directive is concerned with digital currencies and provides provisions concerning the definitions of virtual currencies.

### 5.2.4 Crypto-asset activities and markets in the European Union: Issues, Challenges and Considerations for Regulation, Supervision and Oversight

The article 'Crypto-asset activities and markets in the European Union: Issues, Challenges and Considerations for Regulation, Supervision and Oversight' evaluates the European Union's present regulatory approach to cryptocurrencies. The rapid expansion of cryptocurrencies' ecosystem has intensified the attention of regulatory communities. Regulators are increasingly being challenged to respond fast and appropriately to protect customers, investors and society from crypto-related risks, address the risks themselves and still promote technological advancement in this area.

The article recommends that regulators develop tailored regulatory frameworks that create an environment conducive to the adoption of cryptocurrencies and development of crypto-based commerce, alongside mechanisms to protect the integrity, security and stability of the financial system and its actors. Prudent regulation requires an in-depth understanding of the blockchain technology that underpins cryptocurrencies and its power to revolutionize the global financial system as well as it potential to harm such. Cross-jurisdictional cooperation and government–industry collaboration are essential to a pragmatic global regulatory environment for cryptocurrencies.

### 5.2.5 Digital Currencies and Economic Sanctions: the Increasing Risk of Sanction Evasion

The article ‘Digital Currencies and Economic Sanctions: the Increasing Risk of Sanction Evasion’ evaluates the effects of issuance, widespread adoption, and use of digital currency on economic sanctions. Digital currencies are causing significant disruptions to the existing financial and economic model. Specifically, the article provides important information on sanctions

avoidance and evasion through the use of digital currencies. Digital currencies are more likely to be utilised by persons located in countries that target sanctions. This is the one major limitation associated with a regulatory approach to addressing the problem of sanction evasion.

The article provides some general guidelines that countries can use to at least reduce the risk of sanction evasion through the use of digital currencies. Some of the best practices in this regard are knowing the customer, knowing the transaction and use of contractual safeguards.

### 5.2.6 Financial Crime in the Decentralized Finance (DeFi) Ecosystem: new Challenges for Compliance

The article 'Financial Crime in the Decentralized Finance (DeFi) Ecosystem: new Challenges for Compliance' analyses and evaluates the new challenges for financial crime compliance in the DeFi "world". DeFi is considered to be one of the major steps towards adopting crypto masses. It is expected that DeFi will play a significant role in future and provide the present banking system with a feasible alternative. Therefore, it is crucial that the DeFi industry must address the main risks to ensure its "user" full compliance.

This includes securing the transmission to the appropriate address. This can be achieved by implementing more extensive controls into DeFi apps. In case of price slips and regulatory scrutiny, the De-Fi ecosystem requires regulatory authorities to give stronger assistance. As the DeFi ecosystem is not completely established, the danger of future failures must be minimized by users. Financialization of risks through insurance and controlled intelligent contracting is the last step towards this aim. DeFi initiatives have shown to be effective hacking goals.

The article recommends a joint effort of the DeFi businesses as well as the regulator to achieving the above-mentioned measures.

## 5.3 References


Abreu, E.S. de, Kimura, H. and Sobreiro, V.A., 2019. What is going on with studies on banking efficiency? *Research in International Business and Finance*, [online] 47, pp.195–219. https://doi.org/10.1016/j.ribaf.2018.07.010.

Afzal, A. and Asif, A., 2019. Cryptocurrencies, blockchain and regulation: A review. *The Lahore Journal of Economics*, 24(1), pp.103-130.

Aguiar, S., 2022. *US, UK Are Top Global Money Laundering Hotspots*. WealthBriefingAsisa [online]. Available at: <https://www.wealthbriefingasia.com/article.php?id=193675> [Accessed 16 September 2023]

Ahmad, S., Asghar, M.Z., Alotaibi, F.M. and Awan, I., 2019. Detection and classification of social media-based extremist affiliations using sentiment analysis techniques. *Human-centric Computing and Information Sciences*, [online] 9(1), p.24. https://doi.org/10.1186/s13673-019-0185-6.

Albayati, H., Kim, S.K. and Rho, J.J., 2020. Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. *Technology in Society*, [online] 62, p.101320. https://doi.org/10.1016/j.techsoc.2020.101320.

Al-Hashedi, K.G. and Magalingam, P., 2021. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, [online] 40, p.100402. https://doi.org/10.1016/j.cosrev.2021.100402.

Altikriti, S., Nedelec, J.L. and Barnes, J.C., 2022. The influence of individual differences on the formation of perceptions of risk, social cost, and rewards of crime: A meta-analysis. *Journal of Criminal Justice*, [online] 82, p.101962. https://doi.org/10.1016/j.jcrimjus.2022.101962.

Ardizzi, G., De Franceschis, P. and Giammatteo, M., 2018. Cash payment anomalies and money laundering: An econometric analysis of Italian municipalities. *International Review of Law and Economics*, [online] 56, pp.105–121. https://doi.org/10.1016/j.irle.2018.08.001.

Ariyaluran Habeeb, R.A., Nasaruddin, F., Gani, A., Targio Hashem, I.A., Ahmed, E. and Imran, M., 2019. Real-time big data processing for anomaly detection: A Survey. *International Journal of Information Management*, [online] 45, pp.289–307. https://doi.org/10.1016/j.ijinfomgt.2018.08.006.

Ariyanto, D., Jhuniantara, I., Ratnadi, N., Putri, I. and Dewi, A., 2021. Detecting fraudulent financial statements in pharmaceutical companies: Fraud pentagon theory perspective. *Accounting*, [online] 7(7), pp.1611–1620. Available at: <http://m.growingscience.com/beta/ac/4862-detecting-fraudulent-financial-statements-in-pharmaceutical-companies-fraud-pentagon-theory-perspective.html> [Accessed 12 September 2022].

Arslanian, H. and Fischer, F., 2019. *The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services*. 1st ed. Cham, Switzerland: Springer.

Azinge-Egbiri, N.V., 2021. The International Financial Sector Reform and International Legal Framework for Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Regulation. In: *Regulating and Combating Money Laundering and Terrorist Financing*, [online] Routledge. pp.13–61. https://doi.org/10.4324/9781003017158-2.

Bachmann, G., 2006. *Private Ordnung. Grundlagen ziviler Regelsetzung.* Tuebingen, Germany: Mohr Siebeck.

Baesens, B., Höppner, S. and Verdonck, T., 2021. Data engineering for fraud detection. *Decision Support Systems*, [online] 150, p.113492. https://doi.org/10.1016/j.dss.2021.113492.

Balani, H., 2019. Assessing the introduction of anti-money laundering regulations on bank stock valuation. *Journal of Money Laundering Control*, [online] 22(1), pp.76–88. https://doi.org/10.1108/jmlc-03-2018-0021.

Barboza, F., Kimura, H., Sobreiro, V.A. and Basso, L.F.C., 2016. Credit risk: from a systematic literature review to future directions. *Corporate Ownership and Control*, [online] 13(3), pp.326–346. https://doi.org/10.22495/cocv13i3c2p6.

Barroso, M. and Laborda, J., 2022. Digital transformation and the emergence of the Fintech sector: Systematic literature review. *Digital Business*, [online] 2(2), p.100028. https://doi.org/10.1016/j.digbus.2022.100028.

Basel Committee of Banking Supervison, 2016. Guidelines: Sound management of risks related to money laundering and financing of terrorism, [online] Available at: https://www.bis.org/bcbs/publ/d353.pdf

Beer, D. and Burrows, R., 2013. Popular Culture, Digital Archives and the New Social Life of Data. *Theory, Culture & Society*, [online] 30(4), pp.47–71. https://doi.org/10.1177/0263276413476542.

Bell, R.E., 2002. An Introductory Who's Who for Money Laundering Investigators. *Journal of Money Laundering Control*, [online] 5(4), pp.287–295. https://doi.org/10.1108/eb027309.

Brands, J. and Van Doorn, J., 2022. The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, [online] 127, p.107082. https://doi.org/10.1016/j.chb.2021.107082.

Buchner, B., 2018. Article 1 GDPR paragraph 11. In: Kühling, J. and Buchner, B. (eds.) *Datenschutz-Grundverordnung/BDSG. Legal commentary, 2nd ed.*, Munich, Germany: C.H. Beck.

Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), 2009. *Leaflet „Länderunabhängige Embargomaßnahmen zur Terrorismusbekämpfung“,* [online] Available at: <file:///C:/Users/rawro/Download/afk_merkblatt_embargomassnahmen_terrorismusbekaempfung.pdf> [Accessed 16 August 2023].

Bundesanstalt für Finanzdiensleistungsaufsicht (BaFin), 2020. Financial Action Task Force – FATF, [online] Available at: <https://www.bafin.de/DE/Internationales/GlobaleZusammenarbeit/FATF/fatf_node.html> [Accessed 6 November 2022]

Bughin, J., Chui, M. and Manyika, J., 2017. Clouds, big data, and smart assets: Ten tech-enabled business trends to watch | McKinsey. *McKinsey Quarterly*, [online] Available at: <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/clouds-big-data-and-smart-assets-ten-tech-enabled-business-trends-to-watch> [Accessed 17 September 2022].

Burnes, D., Henderson, C.R., Sheppard, C., Zhao, R., Pillemer, K. and Lachs, M.S., 2017. Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis. *American Journal of Public Health*, 107(8), pp. e13–e21. https://doi.org/10.2105/AJPH.2017.303821.

Byers, P., 2016. *Mitarbeiterkontrollen: Praxis im Datenschutz und Arbeitsrecht*. Munich, Germany: C.H. Beck

Canhoto, A.I., 2021a. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, [online] 131, pp.441–452. https://doi.org/10.1016/j.jbusres.2020.10.012.

Canhoto, A.I., 2021b. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, [online] 131, pp.441–452. https://doi.org/10.1016/j.jbusres.2020.10.012.

Castro, D., 2011. Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising, [online] Available at: <https://d1bcsfjk95uj19.cloudfront.net/files/2011-self-regulation-online-behavioral-advertising.pdf> [Accessed 28 August 2023].

Cassella, D. S., 2018. Toward a new model of money laundering: Is the “placement, layering, integration” model obsolete? *Journal of Money Laundering Control*, 21(4), pp. 494-497.

Chau, D. and Nemcsik, M. van D., 2020. *Anti-Money Laundering Transaction Monitoring Systems Implementation: Finding Anomalies*. 1st ed. Hoboken, New Jersey: Wiley.

Cheng, X., Liu, S., Sun, X., Wang, Z., Zhou, H., Shao, Y. and Shen, H., 2021. Combating emerging financial risks in the big data era: A perspective review. *Fundamental Research*, [online] 1(5), pp.595–606. https://doi.org/10.1016/j.fmre.2021.08.017.

CryptoUK, 2018. *Code of Conduct*, [online] Available at: <https://cryptouk.io/codeofconduct/> [Accessed 28 August 2023].

Dawadi, S., Shrestha, S. and Giri, R.A., 2021. Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, 2(2), pp.25-36.

Däubler, W., Wedde, P., Weichert, T., Sommer, I., 2020. *EU-DSGVO und BDSG*. Frankfurt am Main, Germany: Bund-Verlag.

Däubler, W., 2021. *Gläserne Belegschaften. Das Handbuch zum Beschäftigtendatenschutz. 9th ed.* Frankfurt am Main, Germany: Bund-Verlag.

Deloitte, 2022. *Combatting financial crime in a digital age*, [online] Available at: <https://www2.deloitte.com/ca/en/pages/risk/articles/combatting-financial-crime-in-a-digital-age.html> [Accessed 11 September 2022].

Deutscher Bundestag, Reformbedarf nach der Entscheidung des EuGH zum luxemburgischen Transparenzregister, Opinion PE 6-3000-075/22 of the Scientific Service, 24 January 2023. Available at: <https://www.bundestag.de/resource/blob/934626/1edc22b70d2263a6781331af44e9d231/PE-6-075-22-pdf-data.pdf> [Accessed 16 August 2023].

Diakopoulos, N., 2014. Algorithmic Accountability. *Digital Journalism*, [online] 3(3), pp.398–415. https://doi.org/10.1080/21670811.2014.976411.

Dibrova, A., 2016. Virtual Currency: New Step in Monetary Development. *Procedia - Social and Behavioral Sciences*, [online] 229, pp.42–49. https://doi.org/10.1016/j.sbspro.2016.07.112.

Donfouet, H.P.P., Jeanty, P.W. and Malin, E., 2018. Analysing spatial spillovers in corruption: A dynamic spatial panel data approach. *Papers in Regional Science*, [online] 97(S1), pp.S63–S78. https://doi.org/10.1111/pirs.12231.

Eder, I., 2016. IT-gestützte Abgleiche mit Terrorlisten der EU. In: Wedde, P. (ed.). *Handbuch Datenschutz und Mitbestimmung.* Frankfurt, Germany: Bund-Verlag

EU-Commission, 2015. *The Principles for better self- and co-regulation endorsed in the Better Regulation Package*, [online] Available at: <https://digital-strategy.ec.europa.eu/en/news/principles-better-self-and-co-regulation-endorsed-better-regulation-package> [Accessed 31 October 2022]

European Court of Justice (ECJ), 2001. *Judgment of 18 January 2001, Case C-162/99.* Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61999CC0162> [Accessed 16 August 2023].

European Court of Justice (ECJ), 2022. *Judgment of 22 November 2022, Joined cases C-37/20 and C-601/20*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62020CJ0037> [Accessed 16 August 2023].

Ernst & Young, 2022. *EuGH mit weitreichenden Folgen für die Einsichtnahme in das Transparenzregister. Notice of 1 December 2022*, [online] Available at: <https://www.ey.com/de_de/steuernachrichten/eugh-mit-weitreichenden-folgen-fuer-die-einsichtnahme-in-das-transparenzregister> [Accessed 16 August 2022].

Financial Action Task Force, 2018a. *Mutual Evaluation Report of the United Kingdom - 2018* [online] Paris, France: FATF. Available at: < https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/MER-United-Kingdom-2018.pdf.coredownload.pdf> [Accessed 13 March 2024].

Financial Action Task Force, 2018b. *Financial Flows from Human Trafficking*, [online] Paris, France: FATF. Available at: <https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf> [Accessed 11 September 2022].

Financial Action Task Force, 2022a. *United Kingdom - Follow-up Report & Technical Compliance Re-Rating*, [online] Paris, France: FATF. Available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/fur/Follow-Up-Report-United-Kingdom-2022.pdf.coredownload.inline.pdf> [Accessed 13 March 2024].

Financial Action Task Force, 2022b. *History of the FATF*, [online] Paris, France: FATF. Available at: <https://www.fatf-gafi.org/about/historyofthefatf/#d.en.3157> [Accessed 11 September 2022].

Financial Action Task Force, 2022c. *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, [online] Paris, France: FATF. Available at: <http://www.fatf-gafi.org/media/fatf/documents/Partnering-int-the-fight-against-financial-crime.pdf> [Accessed 11 September 2022].

Financial Action Task Force, 2024. *Frequent Asked Questions*, [online] Paris, France: FATF. Available at: <https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab> [Accessed 13 March 2024].

Financial Conduct Authority (FCA), 2023. Handbook, [online]
Available at: <https://www..handbook.fca.org.uk/handbook/COCON.pdf and https://www. handbook.fca.org.uk/handbook./SYSC/3/2.html> [Accessed 28 August 2023].

Financial Court Dusseldorf (Finanzgericht Düsseldorf), 2011. *Judgment of 1 June 2011, case 4 K 3063/10 Z*, [online] Available at: <https://openjur.de/u/449404.html> [Accessed 14 August 2023].

Financial Intelligence Unit (FIU), 2022. FIU Annual Report 2021, [online] Available at: <https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html> (Accessed 12 November 2022].

<https://www.fstech.co.uk/fst/UK_Comes_Second_Place_For_Global_Money_Laundering.php#:~:text=The%20study%20found%20that%20an,every%20year%20in%20the%20UK>.

Liebetrau, T., 2022. Cyber conflict short of war: a European strategic vacuum. *European Security*, 31(4), pp.497-516.

Loebbecke, C. and Picot, A., 2015. Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems*, [online] 24(3), pp.149–157. https://doi.org/10.1016/j.jsis.2015.08.002.

Macak, M., Daubner, L., Sani, M.F. and Buhnova, B., 2022. Cybersecurity Analysis via Process Mining: A Systematic Literature Review. In: B. Li, L. Yue, J. Jiang, W. Chen, X. Li, G. Long, F. Fang and H. Yu, eds. *Advanced Data Mining and Applications*, Lecture Notes in Computer Science. Cham: Springer International Publishing. pp.393–407. https://doi.org/10.1007/978-3-030-95405-5_28.

Madsbjerg, S., 2017. A New Role for Foundations in Financing the Global Goals. *The Rockefeller Foundation*, [online] Available at: <https://www.rockefellerfoundation.org/blog/new-role-foundations-financing-global-goals/> [Accessed 11 September 2022].

Manuela, C.-C., Maria and Ricardo, M.-C., Nuno, 2020. *Handbook of Research on Cyber Crime and Information Privacy*. Hershey, PA: IGI Global.

Markus, M.L. and Topi, H., 2015. *Big Data, Big Decisions for Science, Society, and Business: Report on a Research Agenda Setting Workshop*. USA: National Science Foundation.

Masciandaro, D., 2017. *Global Financial Crime: Terrorism, Money Laundering and Offshore Centres*. Taylor & Francis.

Masciandaro, D. and Filotto, U., 2001. Money Laundering Regulation and Bank Compliance Costs: What Do Your Customers Know? Economics and the Italian Experience. *Journal of Money Laundering Control*, [online] 5(2), pp.133–145. https://doi.org/10.1108/eb027299.

Maume; P. and Maute, L. 2020. Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offering. Munich, Germany: Verlag C.H. Beck.

May, T. and Bhardwa, B., 2017. The Nature and Structure of Organised Crime Groups Involved in Fraud. In: *Organised Crime Groups involved in Fraud*. [online] Springer International Publishing. pp.57–68. https://doi.org/10.1007/978-3-319-69401-6_4.

Merendino, A., Dibb, S., Meadows, M., Quinn, L., Wilson, D., Simkin, L. and Canhoto, A., 2018. Big data, big decisions: The impact of big data on board level decision-making. *Journal of Business Research*, [online] 93, pp.67–78. https://doi.org/10.1016/j.jbusres.2018.08.029.

Nobel, P., 1987. Gesetz oder private Selbstregulierung? In Dufour, A. (ed.). *Schweizerische Beiträge zum Europarecht. 31*. Genf, Switzerland. pp.441-478.

OECD, 2015. *Industry Self-Regulation: Role and use in supporting consumer interests. Directorate for Science, Technology and Innovations*. Committee on consumer policy. Available at: <https://one.oecd.org/dokument/DSTI/CP(2014)4/FINAL/En/pdf> [Accessed 28 August 2023].

Ofcom, 2008. Criteria for promoting co-and self-regulation, [online] Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0026/38492/co_self_reg.pdf> [Accessed 16 September 2023].

Oppenhoff, 2022. *Öffentlicher Zugang zum Transparenzregister ist europarechtswidrig. Newsletter of 8 December 2022*, [online] Available at: <https://www.oppenhoff.eu./de/news/detail/eugh-oeffentlicher-zugang-zum-transparenzregister-ist-europarechtswidrig/> [Accessed 16 August 2023].

Paschen, U., Pitt, C. and Kietzmann, J., 2020. Artificial intelligence: Building blocks and an innovation typology. *Business Horizons*, [online] 63(2), pp.147–155. https://doi.org/10.1016/j.bushor.2019.10.004.

Pinto, S.O. and Sobreiro, V.A., 2022. Literature review: Anomaly detection approaches on digital business financial systems. *Digital Business*, [online] 2(2), p.100038. https://doi.org/10.1016/j.digbus.2022.100038.

Priebe, T. and Markus, S., 2015. Business information modelling: A methodology for data-intensive projects, data science and big data governance. In: *2015 IEEE International Conference on Big Data (Big Data)*. [online] IEEE. https://doi.org/10.1109/bigdata.2015.7363987.

Randall, L., 2023. *Transparency v privacy – the uncertain future for beneficial ownership registers*. [online] Available at: <https://www.stewardslaw.com/news/transparency-v-privacy-the-uncertain-future-for-beneficial-ownership-registers/> [Accessed 16 August 2023].

Rider, B., 2015. *Research Handbook on International Financial Crime*. Cheltenham, UK: Edward Elgar Publishing.

Rocha-Salazar, J.-J., Segovia-Vargas, M.-J. and Camacho-Miñano, M.-M., 2021. Money laundering and terrorism financing detection using neural networks and an abnormality indicator. *Expert Systems with Applications*, [online] 169, p.114470. https://doi.org/10.1016/j.eswa.2020.114470.

Roßkopf, G., 1999. *Selbstregulierung von Übernahmeangeboten in Großbritannien: Der City Code on Takeovers and Mergers und die dreizehnte gesellschaftsrechtliche EG-Richtlinie*. Berlin, Germany: Dunker & Humblot.

Ruppert, W., 2012. Mitarbeiter-Screening zur Terroristensuche*. Computer und Arbeit (CuA).* 7 – 8, pp. 42-44.

Ryder, N. 2011. *Financial Crime in the 21st Century: Law and Policy*. 6th ed. Cheltenham, UK: Edward Elgar Publishing.

Sadiq, A.S., Faris, H., Al-Zoubi, A.M., Mirjalili, S. and Ghafoor, K.Z., 2019. Chapter 17 - Fraud Detection Model Based on Multi-Verse Features Extraction Approach for Smart City Applications. In: D.B. Rawat and K.Z. Ghafoor, eds. *Smart Cities Cybersecurity and Privacy*, [online] Elsevier. pp.241–251. https://doi.org/10.1016/B978-0-12-815032-0.00017-2.

Saleh, K., Boujarwah, A.A. and Al-Dallal, J., 2001. Anomaly detection in concurrent Java programs using dynamic data flow analysis. *Information and Software Technology*, [online] 43(15), pp.973–981. https://doi.org/10.1016/s0950-5849(01)00199-9.

Schwark, E., 1979. *Anlegerschutz durch Wirtschaftsrecht: Entwicklungslinien, Prinzipien und Fortbildung des Anlegerschutzes, zugleich ein Beitrag zur Überlagerung bürgerlich-rechtlicher Regelung und gewerbepolizeilicher Überwachung durch Wirtschaftsrecht.* Munich, Germany: Verlag C.H. Beck.

Schmid, D., 2018. § 16 Datenschutz. In: Maume, P. and Maute, L. (eds.) *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offering*. Munich, Germany: Verlag C.H. Beck.

Schulz, S., 2018. Artikel 6. In: Gola, P. (ed.) *DS-GVO: Datenschutz-Grundverordnung VO (EU) 216/679*. 2nd ed. Munich, Germany: Verlag C.H. Beck.

Sciurba, M., 2019. 5. The Fight against Money Laundering in the European Union. In: *The Incompatibility of Global Anti-Money Laundering Regimes with Human and Civil Rights*, [online] Nomos Verlagsgesellschaft mbH & Co. KG. pp.77–92. https://doi.org/10.5771/9783748903086-77.

Severino, M.K. and Peng, Y., 2021. Machine learning algorithms for fraud prediction in property insurance: Empirical evidence using real-world microdata. *Machine Learning with Applications*, [online] 5, p.100074. https://doi.org/10.1016/j.mlwa.2021.100074.

Singh, K. and Best, P., 2019. Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, [online] 34, p.100418. https://doi.org/10.1016/j.accinf.2019.06.001.

Song, C., Li, T., Huang, X., Wang, Z. and Zeng, P., 2019. Towards Edge Computing Based Distributed Data Analytics Framework in Smart Grids. In: *Lecture Notes in Computer Science*, [online] Springer International Publishing. pp.283–292. https://doi.org/10.1007/978-3-030-24274-9_25.

Stripling, E., Baesens, B., Chizi, B. and vanden Broucke, S., 2018. Isolation-based conditional anomaly detection on mixed-attribute data to uncover workers' compensation fraud. *Decision Support Systems*, [online] 111, pp.13–26. https://doi.org/10.1016/j.dss.2018.04.001.

Sullivan, K., 2015. Fraud and Anti-money Laundering. In: *Anti–Money Laundering in a Nutshell*, [online] Apress. pp.151–158. https://doi.org/10.1007/978-1-4302-6161-2_9.

Taekema, S., 2021. Methodologies of rule of law research: why legal philosophy needs empirical and doctrinal scholarship. *Law and philosophy*, 40(1), pp.33-66.

Tertychnyi, P., Godgildieva, M., Dumas, M. and Ollikainen, M., 2022. Time-aware and interpretable predictive monitoring system for Anti-Money Laundering. *Machine Learning with Applications*, [online] 8, p.100306. https://doi.org/10.1016/j.mlwa.2022.100306.

The Joint Money Laundering Steering Group (JMLSG), 2023a. *JMLSG Current Guidance*, [online] Available at: <https://www.jmlsg.org.uk/guidance/current-guidance/> [Accessed 16 September 2023].

The Joint Money Laundering Steering Group (JMLSG), 2023b. *JMLSG Guidance: Cryptoassets Transfer ("Travel Rule")*, [online] Available at: < https://www.jmlsg.org.uk/wp-content/uploads/2023/08/Board-approved_JMLSG-Guidance_Part-II-Sector-22-Annex-I_Aug2023.pdf> [Accessed 16 September 2023].

Thommandru, A. and Chakka, B., 2023. Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks. *Sustainable Futures*, [online], 5, p. 100107. https://doi.org/10.1016/j.sftr.2023.100107

Thompson, B.S., 2017. Can Financial Technology Innovate Benefit Distribution in Payments for Ecosystem Services and REDD+? *Ecological Economics*, [online] 139, pp.150–157. https://doi.org/10.1016/j.ecolecon.2017.04.008.

Tiwari, M., Ferrell, J., Geppb, A. and Kumar, K., 2023. Factors influencing the choice of technique to launder funds: The APPT framework. *Journal of Economic Criminology*, [online], 1, p. 100006. https://doi.org/10.1016/j.jeconc.2023.100006

Trujillo, J., Davis, K.C., Du, X., Damiani, E. and Storey, V.C., 2021. Conceptual modelling in the era of Big Data and Artificial Intelligence: Research topics and introduction to the special issue. *Data & Knowledge Engineering*, [online] 135, p.101911. https://doi.org/10.1016/j.datak.2021.101911.

Turki, M., Hamdan, A., Cummings, R.T., Sarea, A., Karolak, M. and Anasweh, M., 2020. The regulatory technology "RegTech" and money laundering prevention in Islamic and conventional banking industry. *Heliyon*, [online] 6(10), p.e04949. https://doi.org/10.1016/j.heliyon.2020.e04949.

United Nations General Assembly, 2019. Take Action for the Sustainable Development Goals. *United Nations Sustainable Development*. Available at: <https://www.un.org/sustainabledevelopment/sustainable-development-goals/> [Accessed 11 September 2022].

United Nations Office of Drugs and Crime, 2019. *Crime Prevention and SDGs*. [online] Available at: <https://www.unodc.org> [Accessed 11 September 2022].

United Nations Office of Drugs and Crime, 2022. *Money Laundering*. [online] Available at: <https://www.unodc.org/unodc/en/money-laundering/overview.html> [Accessed 12 November 2022]

Vandezande, N., 2017. Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review*, [online] 33(3), pp.341–353. https://doi.org/10.1016/j.clsr.2017.03.011.

Varga, S., Brynielsson, J. and Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, [online] 105, p.102239. https://doi.org/10.1016/j.cose.2021.102239.

Von Hippel, E., 1992. *Rechtspolitik: Ziele, Akteure, Schwerpunkte.* Berlin, Germany: Duncker & Humblot.

Wahlers, C., 2011. *Private Selbstregulierung am Beispiel des Kapitalmarktrechts. Vorteile, Nachteile, Optimierung*. Cologne, Germany: V&R unipress

Walker, J., Unger, B., 2009. Measuring Global Money Laundering: "The Walker Gravity Model". *Review of Law & Economics*, [online]. De Gruyter 5(2), pp. 821-853.

Wang, L., Zhang, Z., Zhang, X., Zhou, X., Wang, P. and Zheng, Y., 2021. Chapter One - A Deep-forest based approach for detecting fraudulent online transaction. In: A.R. Hurson and S. Wu, eds. *Advances in Computers*, AI and Cloud Computing, [online] Elsevier. pp.1–38. https://doi.org/10.1016/bs.adcom.2020.10.001.

Wegener, B., 2022. Article 267 AEUV paragraph 51. In: Callies, Ch. and Ruffert, M., eds. *EUV/AEUV mit Europäischer Grundrechtecharta. Legal commentary, 6th ed.* Munich, Germany: C.H. Beck.

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B. and van Ruijven, T., 2021. Understanding incentives for cybersecurity investments: Development and application of a typology. *Digital Business*, [online] 1(2), p.100014. https://doi.org/10.1016/j.digbus.2021.100014.

Whisker, J. and Lokanan, M.E., 2019. Anti-money laundering and counter-terrorist financing threats posed by mobile money. *Journal of Money Laundering Control*, [online] 22(1), pp.158–172. https://doi.org/10.1108/jmlc-10-2017-0061.

White, L., 2022. HSBC to close 114 branches in Britain from April 2023. *Reuters*, 30 November. [Text/HTML]. Available at: <https://www.reuters.com/business/finance/hsbc-close-114-branches-britain-april-2023-2022-11-30/> [Accessed 14 December 2022].

World Bank, 2022. *Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision*. [Text/HTML] World Bank. Available at:

<https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision> [Accessed 14 September 2022].

Wronka, C., 2020. *The relevance of industry self-regulation in light of the principle of subsidiarity enshrined in Art. 5 (3) TEU: Part 1 – Focus on the advertising industry in the UK and Germany*. Beau Bassin, Mauritus: LAP LAMBERT Academic Publishing

Wronka, C., 2022a. Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, [online] 25(1), pp.79–94. https://doi.org/10.1108/JMLC-02-2021-0017.

Wronka, C., 2022b. "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control*, [online] 25(2), pp.330–344. https://doi.org/10.1108/JMLC-04-2021-0035.

Wronka, C., 2022c. Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business. *Journal of Money Laundering Control*, [online] 25(3), pp.656–670. https://doi.org/10.1108/JMLC-06-2021-0060.

Wronka, C., 2022d. Digital currencies and economic sanctions: the increasing risk of sanction evasion. *Journal of Financial Crime*, 29(4), pp.1269-1282. https://doi.org/10.1108/JFC-07-2021-0158.

Wronka, C. 2023, Financial crime in the decentralized finance ecosystem: new challenges for compliance, *Journal of Financial Crime*, 30(1), pp. 97-113. https://doi.org/10.1108/JFC-09-2021-0218

Wronka, C., 2023. Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight. Journal of Banking Regulation, [online] https://doi.org/10.1057/s41261-023-00217-8

Wu, N. and Zhang, J., 2006. Factor-analysis based anomaly detection and clustering. *Decision Support Systems*, [online] 42(1), pp.375–389. https://doi.org/10.1016/j.dss.2005.01.005.

Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M., 2020. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, 77, p.103201.

Zhang, Y. and Trubey, P., 2018. Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. *SSRN Electronic Journal*. [online] https://doi.org/10.2139/ssrn.3161436.

Zimiles, E. and Mueller, T., 2019. *How AI is transforming the fight against money laundering*. [online] Geneva, Switzerland: World Economic Forum. Available at: <https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/> [Accessed 17 September 2022].