Becoming a Monster

-

Analysing the Necessity and Proportionality of Subjecting VASPs to the Ever-Growing Scope of the European Anti-Money Laundering Directive

B.J.G. Loew
LL.M. Law & Technology
ANR:1272063

Supervisor: Dr. Raphaël Gellert
Second Reader: Dr. Robin Pierce

Table of Contents

List of Key Abbreviations

4AMLD	This notation is used specifically to refer to Recitals of Directive 2015/849
5AMLD	This notation is used specifically to refer to Articles of the most recent version of the AMLD, incorporating changes of Directive 2018/843
AML	Anti-Money Laundering
AMLD	Anti-Money Laundering Directive
CDD	Customer due diligence, one of three compliance duties under the AMLD
Charter / CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Directive 2018/843	The amendment of the fourth AMLD. This notation is used to refer to Recitals of this amending Directive.
EDPS	European Data Protection Supervisor
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation
VASP	Virtual Asset Service Provider
WP29	Article 29 Working Party

Table of International Treaties

Convention 108+	Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data* (CETS No. 108 28 January 1981)
Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime	Council of Europe, *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime* (CETS No. 141 8 November 1990)
UN Convention against illicit traffic in narcotic drugs and psychotropic substances	United Nations, *Convention against illicit traffic in narcotic drugs and psychotropic substances* (United Nations Treaty Series vol. 1582, No. 27627 1988)
UNTOC	United Nations, *Convention against Transnational Organized Crime* (adopted by resolution A/RES/55/25 of 15 November 2000)
Terrorist Financing Convention	United Nations, *The International Convention for the Suppression of the Financing of Terrorism* (adopted by resolution 54/109 9 December 1999)
Warsaw Convention	Council of Europe, *Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism* (CETS No. 198 16 May 2005)

Table of EU Legislation

4AMLD	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141/73
CFR / Charter	Charter of Fundamental Rights of the European Union [2012] OJ C 326/391
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
Directive 2018/843	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43

DSM Directive	Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ l 130/92
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1
Open Data Directive	Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56
Law Enforcement Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89
Regulation 1092/2010	Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board [2010] OJ L 331/1
Regulation 2015/847	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 [2015] OJ L 141/1
TEU	Consolidated version of the Treaty on European Union [2012] OJ C 326/01
TFEU	Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/01

Table of case law

Digital Rights Ireland	CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238
Peter Puškár	CJEU Case C-73/16 *Peter Puškár* [2017] ECLI:EU:C:2017:725
S. and Marper	*S. and Marper v UK* App nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008)
Schrems	CJEU Case C-362/14 *Schrems* [2015] ECLI:EU:C:2015:650
Schwarz	CJEU Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670
Tele2 Sverige	CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016] ECLI:EU:C:2016:970

Table of National Legislation

Germany Strafgesetzbuch (StGB)	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 19. Juni 2019 (BGBl. I S. 844) geändert worden ist
Netherlands Wetboek van Strafrecht (Sr)	Wet van 3 maart 1881, Wetboek van Strafrecht, BWBR0001854 (geldend van 1 november 2019

I. Introduction

"He who fights monsters should see to it that he himself does not become a monster" [1]

-

Friedrich Nietzsche

1.1 Problem Statement

In Nietzsche's work a concept that features prominently is the "will to power", or desire to have power.[2] He posited that the will to power is one of the main driving forces in humans, thus explaining a core motive of human behaviour. Power also plays an important role in the contemporary work of Zuboff.[3] Her work explains, from an economic perspective, how the accumulation of (surveillance) data shapes business practices, generates profits and ultimately grants power to the one able to exploit it. Together these two notions offer an interesting and critical backdrop to analyse the regulatory landscape of anti-money laundering and highlight the societal issue that lies at the foundation of this thesis. If people are in fact mainly driven by the desire to have power, and in today's economic reality the most valuable raw resource is in fact surveillance data, there would be a very strong desire, perhaps even an insuppressible urge, to gather as much as possible surveillance data in order to gain and maintain power. However, the negative impact of surveillance being well studied,[4] we can assume that any limitations to our fundamental rights and freedoms, that have been so delicately established in the last century, are carefully considered first and only implemented when truly necessary and proportionate. Or can we?

Human rights arose in the aftermath of the Second World War in an attempt to prevent similar atrocities from recurring and resulted in the drafting of the Universal Declaration of Human Rights (UDHR) in 1948.[5] Included in this Declaration was the right to privacy.[6] As time progressed and processing activities became more common, rights to data protection followed in the 1980s.[7] Though distinct, these two rights to privacy and data protection can be seen as complementary as both aim to protect individual interests, either from state or other actors.

[1] Friedrich Nietzsche, *Jenseits von Gut und Böse. Vorspiel einer Philosophie der Zukunft* (Leipzig, Germany 1886) Aphorisms and Interludes #146

[2] See for instance: Friedrich Nietzsche, *Also sprach Zarathustra: Ein Buch für Alle und Keinen* (Chemnitz, Germany 1883); Friedrich Nietzsche, *Jenseits von Gut und Böse. Vorspiel einer Philosophie der Zukunft* (Leipzig, Germany 1886)

[3] See for instance: Shoshana Zuboff, 'Big Other: surveillance capitalism and the prospects of an information civilization' (2015) 30 Journal of Information Technology 75; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Hachette Book Group 2019)

[4] See for instance: Julie Cohen, 'Surveillance vs. Privacy: Effects and Implications' in David Gray & Stephen E. Henderson (eds), *Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017); Hille Koskela, 'The gaze without eyes: video-surveillance and the changing nature of urban space' (2000) Progress in Human Geography 243; Ivan Manokha, 'Surveillance, Panopticism, and Self-Discipline in the Digital Age' (2018) 16(2) Surveillance & Society 219

[5] Steven McCarty-Snead and Anne Titus Hilby, 'Research Guide to European Data Protection Law' (University of California, Berkeley School of Law 2013) 11

[6] Article 12 UDHR

[7] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data* (28 January 1981)

The origins of anti-money laundering measures, on the other hand, arose out of fear that laundering would be used to channel drug money.[8] By contrast, the aim here is therefore to protect government or public interests from rogue citizen behaviour. Roughly twenty years after the publishing of the UNDHR, the term money-laundering first appeared in print[9] and almost another twenty years later the Financial Action Task Force (FATF) was established by the G-7 Summit in 1989.[10]

Since then it has established and shaped anti-money laundering regulation globally, which has gradually grown in both width and depth as increasingly many industries are subjected to increasingly stricter obligations. This raises the critical question: has the anti-money laundering regulation itself become a monster over time?

1.2 Legal Issue

Since its inauguration the FATF has been very influential in the shaping of global anti-money laundering regulation through the publication of its Recommendations and accompanying Interpretive Notes. These mandate measures that must be taken by its members to counter money laundering in their own jurisdictions. Given that EU Member States form the largest fraction within the international task force, it is therefore not surprising that measures adopted in the FATF Recommendations generally end up in the EU Anti-Money Laundering Directive (AMLD).[11]

As stated earlier, anti-money laundering regulation is continuously growing and in June 2019 the FATF has added its Interpretive Note to Recommendation 15,[12] which "sets out the application of the FATF Standards to virtual asset activities and service providers".[13] As yet another industry has been incorporated in the AML regulatory framework, this offers an important moment to reflect upon the proportionality of these measures before blindly adopting them in the next AMLD.

The AMLD continuously expands its scope under the pretence of protecting society from crime and protecting the stability and integrity of the financial system.[14] However, to avoid function creep it is necessary to critically analyse any expansions to the already far-reaching tentacles of AML regulation and to not automatically accept these as essential. As pointed out by the UN in its report on the right to privacy in the digital age, mass surveillance can have a substantial impact, not only on fundamental rights, but also on the functioning of a vibrant and democratic society as a whole.[15] Furthermore, the Article 29 Working Party has stated that secret,

---

[8] Petrus van Duyne and Michael Levi, *Drugs and Money - Managing the Drug Trade and Crime Money in Europe* (Routledge 2005)

[9] William Gilmore, 'Money Laundering: The International Aspect' in Hector MacQueen (ed) *Money Laundering* (Edinburgh University Press 1993

[10] Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 20 October 2019

[11] See for instance Recital 4 4AMLD; Recital 4 Directive 2018/843; Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261, 264

[12] Financial Action Task Force, 'Information on updates made to the FATF Recommendations ' <http://www.fatf-gafi.org//publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 20 October 2019

[13] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (Paris, updated June 2019) 70

[14] Recital 2 4AMLD

[15] United Nations, 'Resolution 68/167: The right to privacy in the digital age' (A/RES/68/167 adopted 18 December 2013); United Nations Human Rights Office of the High Commissioner, 'Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Room XXI, Palais des Nations, Geneva' <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E> accessed 23 October 2019

massive and indiscriminate surveillance programs are incompatible with our fundamental rights and can only be accepted if the measure is strictly necessary and proportionate in a democratic society.[16] Given the delicate and revelatory nature of financial transactions, it is therefore vital to assess whether the AMLD measures can be justified under current EU data protection legislation.

In June 2019 the FATF added the Interpretive Note to Recommendation 15 to its standards, which makes virtual asset service providers (VASPs) designated, or obliged entities, meaning they are subjected to the anti-money laundering framework. To highlight the legal issues arising from a potential inclusion of VASPs in the AMLD framework, this thesis therefore seeks to analyse, *ex-ante*, the legitimation and justification of subjecting VASPs to the current customer due diligence, monitoring and reporting duties under the AMLD framework.[17]

1.3 Virtual Assets and the Proportionality of Anti-Money Laundering Regulation

Virtual assets are defined by the FATF as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations".[18] This definition will also be adhered to throughout this thesis when referring to virtual assets.[19]

Virtual currencies have been the protagonist in various literature, also in relation to anti-money laundering regulation, however their focus is generally on how to get VASPs to better comply with AML measures.[20] Such publications blindly accept that money laundering is an important public interest that must be pursued.[21] This thesis, however, takes an opposing stance. It builds on critiques expressed about the anti-money laundering regime as a whole. Infringements of fundamental rights have been highlighted often, but are often disregarded.[22] More fundamentally van Duyne illuminates the shaky foundation upon which modern anti-money laundering regulation is based and that this foundation resembles vague assumptions that border more on fiction than on fact.[23] He harshly criticises and warns about the protection of any and

[16] Article 29 Data Protection Working Party, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' (819/14/EN WP 215 10 April 2014) (WP29 Opinion 04/2014) 2

[17] Notably the EBA has warned that simply including certain virtual currency service providers under the AMLD framework does not ensure the imposition of consumer protection or other prudential safeguards. See: European Banking Authority, 'Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)' (EBA- Op-2016-07 2016) 5

[18] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (Paris, updated June 2019) 126

[19] As can be seen, they refer to a broad understanding of assets and exclude "traditional" financial instruments.

[20] See for instance: Niels Vandezande, 'Virtual currencies under EU anti-money laundering law' 2017 33(3) Computer Law & Security Review 341; Mo Egan, 'A Bit(Coin) of a Problem for the EU AML Framework' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan; Clare Chambers-Jones, 'Money Laundering in a Virtual World' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

[21] The shaky foundation of AML regulation will be discussed in Section 4.2.

[22] See for instance: Maria Bergström, 'The Global AML Regime and the EU AML Directives: Prevention and Control' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan; European Data Protection Supervisor, 'Opinion 1/2017 EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications (2017) (EDPS Opinion 1/2017); Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261

[23] Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

every harm, amplified by ever-increasing and intrusive monitoring of citizens, which ultimately results in a cure worse than the alleged threat.[24]

This thesis uses these critiques of the anti-money laundering regime as a starting point. It combines insights from research in virtual assets as well as research in the proportionality of AML measures. In that way it intends to add more critical perspectives to adopting AML measures to VASPs and openly questions the ever-growing scope of the AMLD.

1.4 Research Aim

Governments are tasked with reconciling fundamental but conflicting values such as privacy and data protection with government surveillance to prevent and prosecute crimes.[25] This inherent struggle makes it difficult to promote the agenda of one of these without impacting the other. While money laundering and terrorist financing have been labelled as threats to the single market, it remains important to question certain data processing practices, especially when they so blatantly disregard fundamental rights. The tension between extending enforcement of money laundering on the one hand and upholding constitutional safeguards and fundamental rights on the other hand is continuously rising.[26] Since the digital economy is being heavily promoted in the EU and data transfers encouraged,[27] it is perhaps evermore important to question data transfers and at a larger scale to question measures taken under the pretense of security. The fact that having more data available is handy for a variety of reasons does not justify the disproportionate storage and transmission of such data, which slowly but surely erodes individual's fundamental right to data protection and private life.

The aim of this research is therefore to analyse on which data protection grounds the AMLD obligations can be justified. It raises questions pertaining to existing AMLD practices and critically assesses the necessity and proportionality of subjecting VASPs to these obligations. In this way it aims to highlight known issues of legitimacy and warn of ongoing function creep in the realm of anti-money laundering regulation.

1.5 Research Question

The main research question addressed is whether subjecting VASPs to the AMLD customer due diligence, monitoring and reporting requirements would be proportionate to the aim pursued by the AMLD.[28] To answer this question four sub-questions will be asked. First, do the AMLD obligations respect the GDPR principles of data processing? Second, to what extent do the AMLD obligations respect the rights of data subjects? Third, are the restrictions to individuals' rights to data protection justified under the GDPR? Fourth, are the limitations of the fundamental right to data protection justified?

---

[24] Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality' in Georgios Antonopoulos (ed) *Illegal Entrepreneurship, Organized Crime and Social Control - Studies of Organized Crime* (2016) Springer

[25] Paul de Hert, Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 3

[26] Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261, 293

[27] See for instance: the Digital Single Market (DSM) Directive; the Open Data Directive; Article 1(3) GDPR

[28] Although initially aiming to counter money laundering, the aims of the AMLD have been expanded to include terrorist financing and tax evasion. This expansive scope has been heavily criticised and is further discussed in Section3.2.2.

1.6 Limitations, Methodology and Methods

To assess the proportionality of subjecting VASPs to the AMLD, this thesis will evaluate the customer due diligence, monitoring and reporting requirements set out in the AMLD under the data protection framework of the GDPR. The GDPR gives substance to the fundamental right to data protection enshrined in the Charter,[29] and therefore inferences about the legitimacy of the measures under the GDPR will be relevant to the Charter as well. This thesis will only focus on data protection implications.[30] Furthermore, it will only consider the obligation duties of obliged entities under AMLD and not consider further measures of the AMLD, such as beneficial ownership registers or IBAN registers.[31] It will also not consider the data protection implications of onwards transfers of data to FIUs and competent national authorities.[32, 33] Within Figure 2 (page 11) this thesis can be said to focus on the left hand side of the diagram, specifically the VASP. References are made to FIUs, competent authorities and third parties, however they do not form part of the core of the assessment. Neither do self-regulatory bodies.

In answering the research questions this thesis will employ evaluative, qualitative research methodologies with the goal of producing a normative outcome.[34] This normative legal research broadly aims to study the AMLD measures within the framework of the GDPR.

The evaluative element requires that the obligations, which the VASPs would have to fulfil if they would be included in the AMLD as obliged entities, are analysed within the EU data protection framework to conclude whether the measures are proportional. This is performed in three steps, following the research questions. First, it will be determined whether the obligations adhere to the fundamental principles of data processing laid down by the GDPR, such as data minimisation. Next, it will be assessed to what extent the obligations respect the rights of data subjects, such as the right to information. Finally, it will be evaluated to what extent the limitations on the rights of data subjects are justified.

The qualitative element of the research will consist of doctrinal research, case-law analysis and literature review. EU legislation will be sought in EUR-lex and the FATF website will, in turn, provide its Recommendations. Case-law of the CJEU will be consulted in Curia. Finally, relevant literature will be sought through a multitude of databases, including the Tilburg University library (via WorldCat), ResearchGate, SSRN and Springer. Additionally, opinions of the European Commission, the European Data Protection Supervisor (EDPS) and the former Article 29 Working Party will be consulted via their respective websites.

The goal of employing an evaluative, qualitative research methodology is to produce a normative outcome whether subjecting VASPs to the AMLD obligations is proportional or not. The normative outcome is to be understood as situational (rather than absolute),[35] within the context of established EU data protection legislation as well as case-law.

---

[29] Recital 1 GDPR

[30] The implications of the AMLD measures to other fundamental rights, predominantly the rights to private life and legal remedy, are briefly mentioned in Section 4.3. however will not be discussed in depth, as such an in-depth analysis falls beyond the scope of this thesis which aims to assess the impact from a data protection point of view.

[31] Articles 30 and 32a 5AMLD

[32] See Figure 2

[33] The Law Enforcement Directive will not be considered as it governs data protection at more advanced stages of onwards transfers. The thesis of this scope focusses merely on the initial stage involving obliged entities.

[34] Mark Van Hoecke, *Methodologies of Legal Research - Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2013) v

[35] Mark Van Hoecke, *Methodologies of Legal Research - Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2013) 156-157

1.7 Outline

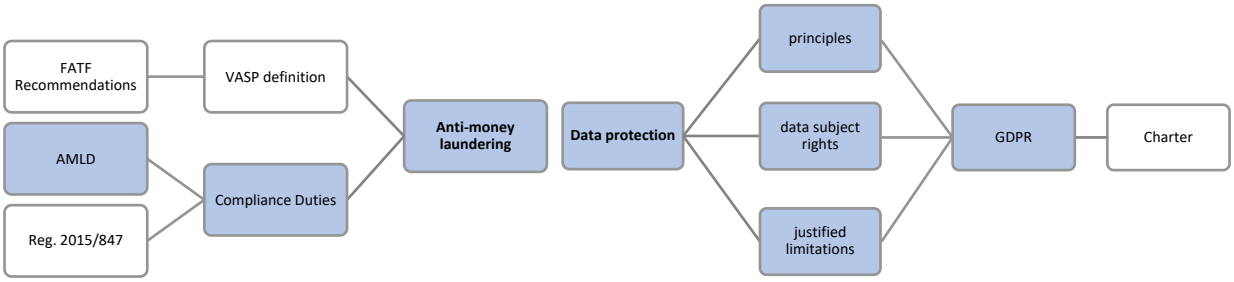
In order to sketch the regulatory landscape, chapter two will discuss the general legal framework. On the one hand this framework is shaped by anti-money laundering regulation, consisting internationally of the FATF Recommendations and within the EU of the AMLD. Additionally, Regulation 2015/847 concerning information accompanying transfers of funds will briefly be covered. Together these instruments shape the compliance obligations central to this thesis. On the other hand, the legal framework is shaped by data protection regulation. The instruments of the Council of Europe and the European Union shaping data protection legislation in the EU will briefly be discussed, namely the ECHR, Convention 108+, the Charter of Fundamental Rights, the GDPR and the Law Enforcement Directive.

Next, chapter three will delve into the GDPR framework by discussing the key principles and data subject rights, while chapter four will assess the permitted restrictions to data subject rights under the GDPR and thereby the limitations of the fundamental right to data protection.

The final chapter will present the research findings of this thesis to conclude that subjecting VASPs to the AMLD customer due diligence, monitoring and reporting obligations is not proportional within the context of EU data protection regulation.

II. Legal Framework

Figure 1: Visualisation of the core legal framework of this thesis



2.1 Introduction

The legal framework within which this thesis operates is defined primarily by the FATF Recommendations, the AMLD and the GDPR. The addition of VASPs to the FATF has triggered this research and so the definition of VASPs under the FATF will be used. The hypothetical scenario of introducing such a definition of VASPs to the current AMLD is at the heart of this thesis and therefore the compliance duties that obliged entities are subjected to will be derived from the AMLD. An additional obligation arises through Regulation 2015/847, which will also be briefly discussed. The data protection part of the legal framework will be provided by the GDPR, which gives substance to the fundamental right to data protection enshrined in the Charter.

This chapter will discuss these depicted instruments, which form the core of this thesis, as well as other influential instruments relevant to the understanding of the legal framework. First the anti-money laundering regulatory framework will be illuminated, followed by data protection.

2.2 Anti-Money Laundering Regulatory Landscape

Anti-money laundering legislation has its origins in the war on drugs. Early international treaties were therefore still bound to offences related to narcotic trade[36] and focused mainly on the seizure of assets,[37] however gradually expanded their scope to include other underlying crimes, also referred to as predicate crimes.[38] Simultaneously identification requirements, record-keeping and monitoring obligations have been introduced.[39] In the meantime, a mostly parallel[40] movement resulted in the International Convention for the Suppression of the Financing of Terrorism.[41] It was adopted to specifically tackle terrorist financing and also built heavily on cooperation with financial institutions. Both schemes have been merged to form a comprehensive surveillance

[36] Art. 3 UN Convention against illicit traffic in narcotic drugs and psychotropic substances
[37] See for instance: Art. 5 UN Convention against illicit traffic in narcotic drugs and psychotropic substances; Chapter III, Section 4: Confiscation, Convention on laundering, search, seizure and confiscation of the proceeds from crime
[38] See for instance: Art. 6(1)(a) UNTOC; Art. 6 Convention on laundering, search, seizure and confiscation of the proceeds from crime
[39] See for instance: Art. 7(1) UNTOC; Arts. 7(2)(c) and 19 Warsaw Convention
[40] Although the preamble of UNTOC explicitly acknowledges the growing links between transnational organized crimes and terrorist crimes, the two remain separate Conventions.
[41] Terrorist Financing Convention

system geared at facilitating various authorities, most notably law enforcement authorities, and, most recently, tax authorities as well.[42] The surveillance is carried out through so called 'obliged entities', which are tasked with compliance duties. While the FATF represents an international cooperation aiming to curtail money laundering, terrorist financing and tax evasion, these aims are incorporated into Union law through the AMLD.

As this thesis is concerned with the potential inclusion of VASPs in the AMLD framework, the largest focus in this chapter will lie on the duties under the AMLD. The obliged entity of interest refers to VASPs and a definition is supplied by the Interpretive Note on FATF Recommendation 15. The compliance duties are supplied mainly by the AMLD, as Regulation 2015/847 mainly concerns requirements already entailed by the customer-due diligence measure of the AMLD. Therefore, there are two critical elements from the anti-money laundering regulatory framework for this thesis: (i) the obliged entity and (ii) the compliance duties.

2.2.1 FATF Recommendations: The Virtual Asset Service Provider (VASP) as Obliged Entity

Under the FATF framework an obliged entity is called 'designated entity' and refers to financial institutions, as well as non-financial businesses and professions, such as casinos, which are listed in FATF Recommendation 22.

In June 2019 the FATF added the Interpretive Note to Recommendation 15 to its standards, which makes virtual asset service providers (VASPs) designated, or obliged entities. It defined VASPs as:

> "any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
>
> i. exchange between virtual assets and fiat currencies;
> ii. exchange between one or more forms of virtual assets;
> iii. transfer of virtual assets;
> iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
> v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset"[43]

where virtual assets are defined as:

> "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."[44]

This definition of virtual assets is extremely far ranging.[45] It includes assets that exclusively exist virtually, such as a house and Linden Dollars in SecondLife, but also virtual assets that can be

[42] See for instance: Article 49 5AMLD; Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (Paris, updated June 2019) 57

[43] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (Paris, updated June 2019) 125

[44] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations' (Paris, updated June 2019) 124

[45] At this point it may be noteworthy to mention that while this thesis is focused on VASPs in their broad FATF definition, a lot of literature referenced to throughout this thesis is focused on virtual currencies, a subset of virtual assets.

transferred into fiat currency, such as Bitcoins.[46] The definition therefore also entails a large array of VASPs, ranging from services providers such as PayPal that exchange fiat currency to virtual currency to service providers that offer, amongst others, closed-scheme virtual currencies such as gold in World of Warcraft.[47]

Under 5AMLD two VASP categories of obliged entities that have been adopted so far are 'exchange providers between virtual currencies and fiat currencies'[48] and 'custodian wallet providers'.[49] Notably these two categories are merely two subsets of the five categories listed by the FATF: (i) currency is more narrow than any type of asset and (iv) custodian wallets are merely one form of safekeeping and administration. Therefore, if VASPs as defined by the FATF were to be taken up in a future version of the AMLD, this would greatly broaden the scope of obliged entities. It would incorporate entire industries currently not subjected to the burdensome compliance duties and give rise to a variety of concerns discussed in the upcoming chapters.

2.2.2 The Anti-Money Laundering Directive (AMLD)

The Anti-Money Laundering Directive essentially transposes the FATF Recommendations into Union law.[50] It proclaims to use a risk-based approach, according to which greater risks require greater interference and action.[51] Furthermore, it outlines various duties and obligations that obliged entities and Member States must adhere to. The focus of this thesis are the compliance duties that obliged entities must fulfil, namely customer due diligence, monitoring obligations and reporting obligations.

2.2.2.1 Customer Due Diligence (CDD)

Customer due diligence measures are included in Chapter II of the AMLD and pertain, roughly speaking, to knowing your customer. The obligation is triggered when commencing a business relationship,[52] when an occasional transaction above a certain threshold is carried out,[53] when suspicion of money laundering exists[54] or when there are doubts about the veracity or adequacy of customer identification data.[55,56] The obligation consists of four main parts, namely (i) identifying the customer,[57] (ii) identifying and verifying the beneficial owner,[58] (iii) assessing and obtaining information on the intended nature of the business relationship[59] and (iv) retaining any

[46] Clare Chambers-Jones, 'Money Laundering in a Virtual World' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan 166
[47] Niels Vandezande, 'Virtual currencies under EU anti-money laundering law' 2017 33(3) Computer Law & Security Review 341, 342
[48] Article 2(1)(3)(g) 5AMLD
[49] Article 2(1)(3)(h) 5AMLD
[50] Recital 4 4AMLD
[51] See for instance: Recital 3 4AMLD; Articles 4, 6, 7, 9, 12 5AMLD; EDPS Opinion 1/2017, para 13. In practice, however, almost everything is labelled high risk and the instrument itself does not always adhere to this principle. For a critical assessment of the risk-based approach under the AMLD see: Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan
[52] Article 11(a) 5AMLD
[53] Article 11 5AMLD: (b)(i) a transaction > €15,000; (b)(ii) a wire transfer > €1,000; (c) someone trading in goods receiving cash > €10,000; (d) providers of gambling services a transaction > €2,000
[54] Article 11 (e) 5AMLD
[55] Article 11(f) 5AMLD
[56] Although these last two are heavily critiqued due to their subjective nature
[57] Article 13(1)(a) 5AMLD
[58] Article 13(1)(b) 5AMLD
[59] Article 13(1)(c) 5AMLD

documentation and information which are necessary to fulfil the above-mentioned requirements for a minimum of five years and up to ten years after the end of the business relationship.[60]

In scenarios where the customer is a natural person identification can occur through documentation, such as a passport, or, since the 2018 update, also via secure remote or electronic means that are approved and accepted by the relevant national authorities.[61] In such scenarios it is probable that the customer is also the beneficial owner. However, in the scenario where the customer is a company, trust or foundation, identifying the customer will lead to a legal person. Therefore, identification of the beneficial owner is required to ultimately still lead to a natural person. In either scenario the obliged entity is able to identify its customer.[62]

The identification and verification are obtained from reliable and independent sources,[63] such as a passport issuing authority, and must occur before or during the establishing of a business relationship, or as soon as reasonably practicable. If verification is not possible the business relationship must be ended.[64]

2.2.2.2 Monitoring

The second main type of compliance duty that obliged entities must pursue is the ongoing monitoring of their business relationship. The entity must apply specific scrutiny that transactions are consistent with their knowledge of their customer and risk profile as well as ensure that information is kept up-to-date.[65]

2.2.2.3 Reporting Obligation

Finally, the third main type of compliance duty consists of a reporting obligation. This duty entails that obliged entities must act on their own initiative in cases where they know, suspect or have reasonable grounds to suspect that funds (regardless of their amount) are proceeds of a criminal activity or related to terrorist financing. Additionally, suspicious transactions (including attempted transactions) must be reported. Besides acting on their own initiative the reporting obligation also entails that obliged entities cooperate with Financial Intelligence Units (FIUs) by replying promptly to their requests and providing all necessary information.[66] While this duty aims to foster the cooperation between obliged entities and FIUs, the very broad and not further specified vocabulary, such as 'all relevant information' or 'suspicious' transactions, is particularly worrisome.

2.2.2.4 Supervision under the AMLD

Besides the compliance duties of obliged entities, another aspect of the AMLD framework that is particularly critical its supervision system. This is because applicable data protection regulation changes while information passes through this web of supervision.[67]

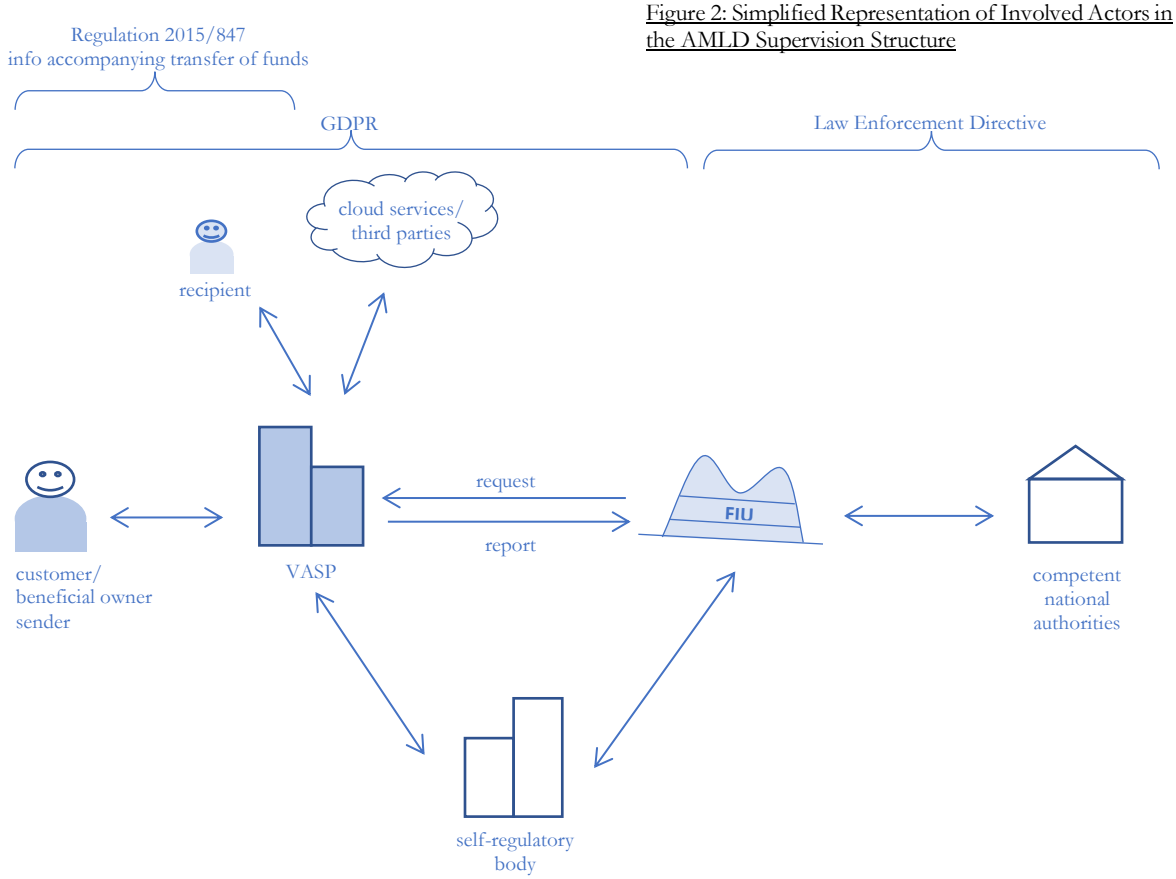
In this system obliged entities form the first 'guard post' and act as contact point with the 'outer world' by screening and monitoring their customers. Under their reporting obligation this information then enters the supervision web of the AMLD, with Financial Intelligence Units

[60] Article 40(1)(a) 5AMLD
[61] Article 13(1)(a) 5AMLD
[62] Following Articles 15 – 18a 5AMLD simplified and enhanced customer due diligence may exist, respectively, depending on the risk of individual customers or entire regions (or third countries). These variations will not be explored in depth in this thesis as they do not take away from the essence of this obligation to identify and verify the identity of a customer, and potentially a beneficial owner.
[63] Article 13(1)(a) 5AMLD
[64] Article 14 5AMLD
[65] Article 13(d) 5AMLD
[66] Article 33 5AMLD
[67] The Law Enforcement Directive is applicable for any data processing performed by law-enforcement or other entities entrusted to exercise such powers while the GDPR applies to any data processing not performed by such a public or publicly entrusted entity. This can clearly be seen in Figure 2.

(FIUs) as first recipient of information. The FIUs are specifically set up to detect, prevent and combat money laundering and terrorist financing.[68] Their main tasks lie in requesting, analysing and disseminating suspicious transaction reports and other information relevant to money laundering and/or terrorist financing.[69] In order to do this they rely on information provided by obliged entities, but are also able to initiate their own investigations and take urgent action independently or together with other FIUs.[70] The FIUs, in turn, also function as a middle man between obliged entities and competent national authorities, such as law enforcement- or tax authorities.[71] Competent authorities are thus the next actor in the information chain. They cover a wide array of authorities, including law enforcement,[72] banking,[73] anti-corruption and tax authorities.[74]

These authorities, in turn are part of larger European network of cooperation, which includes the European Supervisory Authorities (ESAs).[75] Together with the European Commission and the European Central Bank Council, the ESA forms the European Systemic Risk Board (ESRB).[76] Figure 2 below summarizes the basic structure of this web of data transmission between the different involved actors.

Figure 2: Simplified Representation of Involved Actors in the AMLD Supervision Structure



[68] Article 32(1) 5AMLD
[69] Recital 37 4AMLD; Article 32(3) 5AMLD
[70] Article 32 5AMLD
[71] Article 49 5AMLD
[72] Article 49 5AMLD
[73] Recital 23 juncto Article 48(3) 4AMLD
[74] Recital 44 5AMLD
[75] The European Supervisory Authorities consist of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA). See also: Recital 23 4AMLD
[76] The ESRB is concerned with the macro-prudential oversight of the EU financial system in order to prevent or mitigate systemic risk. See: Article 3(1) Regulation 1092/2010; European Securities and Markets Authority, 'European

2.2.3 Regulation 2015/847: Information Accompanying Transfers of Funds

Besides the three main compliance duties mentioned earlier, another duty exists linked specifically to the transfer of funds. Regulation 2015/847 builds on FATF Recommendation 16, which is concerned with wire transfers,[77] and sets out rules regarding the transfers of funds and the information that must accompany these transfers. The Regulation identifies three types of involved payment service providers, each expected to perform slightly different roles throughout the transfer, especially relating to the verification of the accuracy of provided information.

The first identified party is the payment service provider of the 'sender' of funds. This service provider must record[78] and verify[79] the name of the payer, their account number and either their address, official personal document number (such as a passport number), customer identification number or date and place of birth. Additionally, the name and account number of the recipient must be recorded.[80] This set of information is akin to the customer due diligence information required under the AMLD.[81]

The second party distinguished by the Regulation is the is the payment service provider of the 'recipient' of funds. This service provider must check whether the information accompanying the transfer is complete[82] and is responsible to verify the name and account number of the 'recipient' in cases of transfers exceeding €1,000.[83]

The final category of involved party refers to intermediary payment service providers, which are tasked with the detection of missing information. They must check whether the correct fields have been filled in with admissible inputs, but are not tasked with any form of verification.[84] In cases of missing information they may reject a transfer wholly, or request the missing information, either before or even after transmitting the transfer of funds.[85]

Since the core of Regulation 2015/847 revolves around identification it overlaps with the CDD requirement under the AMLD and will therefore not be covered separately in this thesis. Implications of CDD measures also apply to the requirements under Regulation 2015/847.

Supervisory Framework' <https://www.esma.europa.eu/about-esma/governance/european-supervisory-framework> accessed 1 November 2019

[77] Recital 3 Regulation 2015/847

[78] Article 4(1) Regulation 2015/847

[79] Article 4(4) Regulation 2015/847

[80] Article 4(2) Regulation 2015/847

[81] Notwithstanding these information requirements, certain scenarios exist in which all of this information is not necessary, at least not initially. One such case exists where all involved service providers are established in the EU. In such circumstances it is possible to only provide the account numbers of both the 'sender' and the 'recipient', however the additional information must still be available upon request. Similarly, for transfers with a 'recipient' located outside the EU and a transfer below €1,000, the name and account numbers suffice. See also: Articles 5(1); 5(2); 6(2) Regulation 2015/847

[82] Article 7(2) Regulation 2015/847

[83] Article 7(3) Regulation 2015/847

[84] Article 11 Regulation 2015/847

[85] Article 12(1) Regulation 2015/847

2.3 Data Protection Regulatory Landscape

2.3.2 The Charter of Fundamental Rights (CFR)

With the entry into force of the Lisbon Treaty in 2009, the right of data protection was enshrined as a fundamental right in the Charter of Fundamental Rights (CFR),[86] where Article 16 of the Treaty on the Functioning of the European Union (TFEU) created a new legal basis for the EU to legislate on data protection matters.[87] Together these instruments form crucial pieces of primary legislation establishing the right to data protection within the EU.

The fundamental right to data protection is enshrined in Article 8 of the Charter, which grants everyone the right to the protection of personal data concerning them,[88] as well as requiring that data must be processed fairly, for specified purposes, and on grounds of a legitimate basis.[89] Limitations to the fundamental right to data protection must be provided for by law, respect the essence of the right to data protection and be necessary and proportionate. Additionally, limitations must protect the rights and freedoms of others or meet objectives of general interest recognised by the Union.[90,91]

The fundamental rights enshrined in the Charter are given effect through secondary legislation such as the GDPR.

2.3.3 The General Data Protection Regulation (GDPR)

The first attempt to enshrine the fundamental rights of the Charter was made through the Data Protection Directive (DPD), adopted in 1995.[92] It attempted to harmonize data protection law at the national level.[93] 21 years later the way data is collected, used and abused has changed substantially and so an overhaul of data protection legislation was in order. Having entered into force on 25 May 2018, the General Data Protection Directive (GDPR) built on the DPD as well as primary legislation discussed earlier, elevating the level of harmonization as it comes in the form of a Regulation instead of a Directive. The GDPR has modernised the regime to address the modern digital age's economic and social challenges.[94]

This thesis will follow the structure of the GDPR and first analyse whether the AMLD adheres to the fundamental data processing principles. Next, it will assess to what extent the obligations respect the rights of data subjects and finally it will be evaluated whether the limitations imposed on the rights of data subjects are justified.

Article 5 GDPR lists the principles that must be adhered to when processing personal data. Data must be (i) processed lawfully, fairly and transparently, (ii) limited to a specific purpose, (iii) minimized to what is necessary for a specific purpose, (iv) accurate, (v) not kept for longer than necessary, (vi) be handled with integrity and confidentiality and finally (vii) the controller must

---

[86] Article 8(1) CFR
[87] Article 16(1) TFEU
[88] Article 8(1) CFR
[89] Article 8(2) CFR
[90] Article 52(1) CFR
[91] These objectives of general interest refer to Article 3 of the Treaty on European Union (TEU) and include the promotion of peace, freedom, security, justice and the well-being of its peoples, as well as the internal market.
[92] Article 34 Data Protection Directive
[93] Until then the different legal regimes had given effect differently to Convention 108. Drafted by the Council of Europe, it remains in force and even to this day Convention 108+ is the only international treaty on data protection. For more on this see for instance: European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018) XX
[94] European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018) 30

demonstrate compliance with these principles. In Section 3.2 it will be assessed whether these principles are adhered to.

Next are the rights of the data subjects, which are contained in Chapter III of the GDPR and consist of the right to transparency, which entails the right to information and the right to access, the right to rectification, to erasure, to request the restriction of processing, to data portability, the right to object processing and to not be subject to automated decision making.[95] Additionally data subjects have the right to remedies, which are contained in Chapter VIII.[96] The impact of the AMLD measures on the rights of data subjects will be assessed in Section 3.3.

As these rights are not absolute, limitations to these rights will be assessed next. Since the GDPR gives substance to the right to data protection enshrined in the Charter, it is not surprising that the requirements permitting limitations are very similar. Due to this similarity in requirements between the GDPR and the Charter, this section will serve as foundation for the proportionality of AMLD measures, both under the GDPR, as well as under the Charter. Limitations to the right to data protection under both the GDPR and the Charter must (i) respect its essence, (ii) be a necessary and proportionate measure in a democratic society and must (iii) aim to safeguard one of ten listed objectives, amongst which are the prevention, investigation, detection or prosecution of criminal offences as well as monitoring functions carried out in this pursuit.[97] In addition, several specific provisions must be taken up in such a limiting law, including the categories of personal data affected, the specification of controllers, the storage periods for such data and any applicable safeguards.[98]

2.3.4 The Law Enforcement Directive

As its name suggests, the Law Enforcement Directive (Directive 2016/680) specifically addresses the processing of personal data in the realm of law enforcement activities. It therefore applies exclusively to authorities that are engaged in such activities. These are either public authorities or other bodies or entities entrusted with public authority and powers. This Directive can be seen on the right side of Figure 2 and lays down the rules of data processing for such public law enforcement authorities. Although it is beyond the scope of this thesis, it is interesting to note that the general principles governing data processing under the Law Enforcement Directive are very similar to those of the GDPR.[99] However, transparency is omitted and the principles of data minimisation and purpose limitation must be applied flexible as not to render legitimate surveillance operations completely ineffective.[100] Due to the nature of law enforcement activities, the rights of data subjects are severely more restricted than those under the GDPR. To this effect data subjects do have the right to information and access on paper, however these may be restricted partly or wholly.[101] Similarly, the rights to rectification and erasure may be restricted partly or wholly, and sometimes be effectuated merely as a restriction of data processing, for instance when the data must be maintained for purposes of evidence.[102]

---

[95] Articles 12-22 GDPR
[96] Articles 77-82 GDPR
[97] In comparison the Charter requires that limitations are provided for by law, respect the essence of fundamental rights, are necessary and proportionate and either pursue recognized objectives of general interest in the EU or protect the rights and freedoms of others. See Article 52(1) CFR.
[98] Article 23 GDPR
[99] Article 5 GDPR: personal data must be processed (i) lawfully, fairly and transparently, (ii) limited to a specific purpose, (iii) minimized to what is necessary for a specific purpose, (iv) accurate, (v) not kept for longer than necessary, (vi) be handled with integrity and confidentiality and finally (vii) the controller must demonstrate compliance with these principles.
[100] European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018) 283
[101] Articles 12-15 Law Enforcement Directive
[102] Article 16 Law Enforcement Directive

III. Principles of Data Processing & Data Subject Rights

3.1 Introduction

The first attempt to enshrine the fundamental rights of the Charter was made through the Data Protection Directive (DPD), adopted in 1995.[103] It attempted to harmonize data protection law at the national level. Until then the different legal regimes had given effect differently to Convention 108. 21 years later the way data is collected, used and abused has changed substantially and so an overhaul of data protection legislation was in order. Having entered into force on 25 May 2018, the General Data Protection Directive (GDPR) built on the DPD as well as primary legislation discussed earlier, elevating the level of harmonization as it comes in the form of a Regulation instead of a Directive. The GDPR has modernised the regime to address the digital age's economic and social challenges.[104]

This chapter will analyse how and to what extent the measures under the AMLD and Regulation 2015/847 adhere to the fundamental principles of data processing enshrined in the GDPR. The fundamental principles of data processing are important as they must be adhered to, especially in the context of surveillance measures.[105] Next, it will consider which data subject rights are impacted and how they are curtailed through the AMLD measures. This chapter therefore seeks to answer the first two research questions, namely do the AMLD obligations respect the principles of data processing? And, to what extent do the AMLD obligations respect the rights of data subjects?

3.2 Principles of Data Processing

Article 5 GDPR lists the principles that must be adhered to when processing personal data. Data must be (i) processed lawfully, fairly and transparently, (ii) limited to a specific purpose, (iii) minimized to what is necessary for a specific purpose, (iv) accurate, (v) not kept for longer than necessary, (vi) be handled with integrity and confidentiality and finally (vii) the controller must demonstrate compliance with these principles. In the upcoming sub-sections, it will be assessed whether each of the three main compliance duties that VASPs must adhere to respect the principles of data processing laid down in the GDPR.

3.2.1 Lawfulness, Fairness and Transparency

The first principle of data processing is trifold, requiring that data is processed lawfully, fairly and transparently. The GDPR distinguishes between special categories of personal data and other personal data. Special categories of personal data refer to data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership", as well as "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".[106] The

[103] Article 34 Data Protection Directive
[104] European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018) 30
[105] WP29 Opinion 04/2014
[106] Article 9(1) GDPR

processing of such data is in principle forbidden, unless one of the ten conditions mentioned in Article 9(2) GDPR is met.[107] On the other hand, processing personal data that does not fall under the category of special data is generally permissive and must fulfil one of the six grounds listed in Article 6 GDPR.[108] The AMLD posits that processing of personal data within its realm should be seen as a matter of public interest.[109] As the EDPS has pointed out, "EU legislation is often required to meet several public interest objectives which may sometimes be contradictory and require a fair balance to be struck between the various public interests and fundamental rights protected by the EU legal order."[110] The public interests at play with the AMLD are the prevention of crime, which stand starkly at odds with the fundamental rights to data protection and private life. As is discussed in Section 4.2, it is highly questionable whether the aims of the AMLD can truly be considered to be in the public interest.

The principle of transparency requires that data subjects are informed about the processing operation and its purposes.[111] Information therefore has to be provided in clear and plain language and be able to make data subjects aware of the risks, rules and safeguards of processing, as well as their rights.[112]

Finally, the principle of fairness goes beyond transparency, requiring that it is made possible for data subjects to truly understand what is happening with their data. On top of that the requests of data subjects must be adhered to and in general fairness implies an ethical treatment of the data.[113]

3.2.1.1 Customer Due Diligence (CDD)

The customer due diligence (CDD) requirement is triggered when commencing a business relationship,[114] when an occasional transaction above a certain threshold is carried out,[115] when suspicion of money laundering exists[116] or when there are doubts about the veracity or adequacy of customer identification data.[117,118]

The verification and identification of customers and beneficial owners entails several data processing activities within the meaning of the GDPR.[119] When the initial identifying information is obtained from a customer it is collected and recorded. In some cases, verification may also entail the transmission to an independent authority for verification. Afterwards this data is stored internally and thus organised and perhaps even structured. Finally, when the business relationship ends, the data is erased. The simple act of verification may therefore already count three types of processing activities.

The verification of identification of natural persons will most likely occur via a government issued piece of identification, such as a passport or an ID-card. Passports contain pictures, and

---

[107] Article 9(2) GDPR
[108] Article 6(1) GDPR, they are: (a) the consent of the data subject, (b) the processing is necessary for the performance of a contract, (c) for the compliance with a legal obligation of the controller, (d) to protect the vital interests of the data subject or another natural person, (e) for the performance of a task in the public interest, or (f) for the legitimate interests pursued by the controller.
[109] Article 43 5AMLD
[110] European Data Protection Supervisor, 'Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (2019) (EDPS Proportionality Guidelines) 3
[111] Article 12 GDPR
[112] Recital 39 GDPR
[113] European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018) 118-119
[114] Article 11(a) 5AMLD
[115] Article 11 5AMLD: (b)(i) a transaction > €15,000; (b)(ii) a wire transfer > €1,000; (c) someone trading in goods receiving cash > €10,000; (d) providers of gambling services a transaction > €2,000
[116] Article 11 (e) 5AMLD
[117] Article 11(f) 5AMLD
[118] Although these last two are heavily critiqued due to their subjective nature
[119] Article 4(2) GDPR

newer ones biometric data such as fingerprints. Depending on the exact mechanisms of verification by the VASP, the verification stage may therefore entail collecting, recording and storing a digital copy of the passport in their system.[120] Picture scans may allow the identification of someone's race or ethnic origin and digital reading of passports may allow the identification of someone's biometric data. In such cases this form of processing therefore falls within the scope of Article 9 GDPR[121] and is in principle forbidden.

Processing of such special data may be granted, however, as long as it "is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[122] Chapter 4 will address these matters in more detail, demonstrating that processing under the AMLD cannot be considered to meet those requirements.

Alternatively, obliged entities may therefore want to make use of third-party verification services, such as WebID. In cases where the verification occurs externally through an intermediary and all other instances where the VASP only processes non-special personal data, Article 6 GDPR in conjunction with the AMLD applies to establish the lawful basis for processing.[123] Under this regime the processing may be legitimized on the basis of fulfilling a legal obligation outlined by the AMLD,[124] pursuing a matter of public interest,[125] or a legitimate interest of the obliged entity[126] in the form of wanting to know who one's customers are and having the ability to address them.

As Chapter 4 will establish, the lawfulness of the AMLD is shaky making that an ill-fit ground on which to process data. Similarly, it is highly questionable whether the aims pursued by the AMLD truly pursue a public interest and therefore this ground also falls away. Therefore, for customer due diligence matters, only the legitimate interest ground remains. Next to lawfulness, data should also be processed fairly and transparent. This must be ensured by every controller and processor individually. Overall, the main concern at the CDD stage relates to the lawfulness of any special categories of personal data.

3.2.1.2 Monitoring

The second type of compliance duty that obliged entities must pursue is the ongoing monitoring of their business relationship, including the scrutiny of transactions undertaken throughout the course of that relationship.[127]. Therefore, the data is being recorded, or put on file. In order to do so it is highly likely that the data will also be organized and perhaps even structured so that it can be easily retrieved in the internal IT system. As the AMLD also requires to keep these files for a minimum of five years,[128] this entails the storage of data for long periods of time. In this time the data is likely to be retrieved, consulted and used, and perhaps even adapted or altered to add or amend certain information. Therefore, up to ten processing activities can arise out of this compliance duty and its broad reach makes it akin to a blanket surveillance measure.

Given the vast array of processing activities entailed by this compliance duty, it is perhaps unsurprising that issues may emerge, especially regarding the processing of special categories of personal data. This may be in relation to transactions to certain organizations that may directly

[120] However, this is not necessary (see Art. 27 AMLD). Verification may also occur through a third party such as WebID, so that the VASP only receives a green or red light depending on whether the beneficiary owner has been identified and verified. In such cases the third party will need to be able to provide relevant copies of identification and verification data upon requests from authorities.
[121] Article 9(1) GDPR
[122] Article 9(2)(g) GDPR
[123] See also: Recital 45 GDPR
[124] Article 6(1)(c) GDPR
[125] Article 43 5AMLD
[126] Article 6(1)(f) GDPR
[127] Article 13(d) 5AMLD
[128] Article 40(1)(a) 5AMLD

reveal special categories of personal data, such as adherence to a specific political party or a person's sexual orientation and sex life. Political party adherence may be revealed through transfers of funds to specific parties. The pan-European party 'Volt', for instance, accepts donations via PayPal,[129] a VASP under the FATF definition as it exchanges virtual with fiat currencies. Similarly, sexual orientation and/or sex life may be revealed through transactions to adult entertainment services. An example would be payments made via the 'Verge' cryptocurrency, accepted by adult entertainment giant Mindgeek.[130] Here it can be argued that for such delicate matters many people may in fact choose VASPs over traditional financial services to protect their identity and secure their privacy, [131] especially in less liberal societies. Therefore, including VASPs into the scope of the AMLD could have a large impact on personal development in such scenarios where individuals have specifically chosen to protect their privacy. Hence, the lawfulness of the monitoring obligation must at this stage be summarized to be at least questionable.

Next to lawfulness, data should also be processed fairly and transparent. The structural and blanket nature of this surveillance measure deem it unfit to qualify as a truly fair or transparent measure and therefore, here too, a red flag is raised. While there may be some merit to the argument that surveillance is futile when the subject is being informed, it is also important to note the context in which this occurs. In the context of a surveillance mission performed by secret services or regarding a criminal it may be more appropriate to curtail rights of data subjects, however when people are being subjected to constant surveillance even where there is no evidence of suggesting that their conduct might have a link with serious crime this is clearly problematic.[132] It severely undermines the principle of being innocent until proven guilty and thus endangers the rule of law.

3.2.1.3 Reporting Obligations

The third main type of compliance duty consists of a reporting obligation. This obligation entails that obliged entities act on their own initiative in cases where they know, or have reasonable grounds to suspect money laundering or terrorist financing and additionally report such suspicious transactions to their national FIU. Vice versa, if an FIU requests information, obliged entities must share it.[133] This therefore entails at least two data processing activities, namely transmission and disclosure.

Assessing the lawfulness of the reporting obligations, a base is questionably given in law through the AMLD,[134] however it is important to note that the reporting obligation also arises when there is a suspicion of money laundering or terrorist financing, without explaining on what grounds such a suspicion may arise.[135] It remains questionable whether such subjective judgments amount to "sufficient indications to assume that the data subjects are rightly" under surveillance.[136] On a national level indicators are established that may guide the decision-making of obliged entities in this regard, however in practice these often boil down to a subjective judgment being made.[137]

---

[129] Volt Detschland, 'Unterstütze Volt Deutschland' <https://www.voltdeutschland.org/spenden> accessed 3 November 2019

[130] Chris Morris, 'Porn Partnership Pumps This Cryptocurrency Up 22%' (*Fortune*, 17 April 2018) <https://fortune.com/2018/04/17/verge-pornhub-mindgeek-cryptocurrency-brazzers/> accessed 3 November 2019

[131] Niels Vandezande, 'Virtual currencies under EU anti-money laundering law' 2017 33(3) Computer Law & Security Review 341, 352

[132] This line of reasoning also played a central role in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238 (*Digital Rights Ireland*), see especially para 58

[133] Article 33 5AMLD

[134] Recital 45 GDPR; see also: Chapter 4

[135] Article 33(1)(a) 5AMLD

[136] CJEU Case C-73/16 *Peter Puškár* [2017] ECLI:EU:C:2017:725 (*Peter Puškár*) para 117

[137] See for instance the Dutch indicators: Financial Intelligence Unit - Nederland, 'Meldergroepen' <https://www.fiu-nederland.nl/nl/Meldergroepen> accessed 29 October 2019

Deciding on what suspicious constitutes is therefore left up to the discretion of obliged entities, resulting in the fundamental rights of individuals being *de facto* arbitrarily limited. This undoubtedly raises concerns of both legal certainty, as well as the rule of law. On top of that, clients of VASPs are not informed when their data is being transmitted to a national FIU,[138] and they may even have their rights to access curtailed.[139] Since there is no legal standard that is being adhered to and suspicious reports can be triggered at random, the circumstances under which reporting occurs are highly critical. By employing a hit-and-miss technique, individuals with no links to serious crime may become entangled in the invasive surveillance network of the AMLD, subjected to scrutiny by FIUs and various public authorities. The undesirability of expanding such practices to a seemingly never-ending list of professions and therefore individuals is evident and not only gravely undermines the fundamental rights framework, but outright disregards it.

3.2.2 Purpose Limitation

The principle of purpose limitation entails that data is collected for a specified, explicit and legitimate purpose and not further processed in a manner incompatible with those purposes.[140] This results in four requirements to be fulfilled for the purpose limitation principle. The legitimacy was already questioned in Section 3.2.1 and further developed in Section 4.2. The requirements of specific and explicit require that purposes are narrowed down as far as possible to avoid unnecessary broad or vague statements.

3.2.2.1 Customer Due Diligence

Since customer due diligence entails mainly the identification and verification of customers,[141] the purpose of processing data is given by the goal to identify the customer. This goal is specified and made relatively explicit, albeit indirectly, in the AMLD. Once customers are identified, there is no reason to further process personal data at this particular stage. It can therefore be concluded that at this particular stage no new concerns arise regarding the AMLD duty for obliged entities to identify and verify their customers.

3.2.2.2 Monitoring

At the monitoring stage, however, concerns start appearing in the form of major criticisms concerning the purpose limitation of the AMLD as a whole. The AMLD explicitly mentions that data processing for other purposes than its main objectives is prohibited,[142] however its purpose is defined extremely broad in the AMLD: "to prevent the use of the financial system for the purposes of money laundering and terrorist financing".[143] It is thus already questionable whether such a broad purpose really follows the ethos of purpose limitation and criticism has been expressed that money laundering and terrorist financing are distinct phenomena that cannot be approached with the same "catch-all" toolkit.[144] Measures appropriate for emergency situations relating to terrorist financing are quick to be found excessive for less time-sensitive matters such as money laundering or tax evasion.[145] The inclusion of tax evasion has also been heavily

[138] Article 39 5AMLD
[139] Article 41(4) 5AMLD
[140] Article 5(1)(b) GDPR
[141] Article 13 5AMLD
[142] Article 41(2) AMLD
[143] Article 1(1) AMLD
[144] Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261, 271
[145] EDPS Opinion 1/2017, para 51

criticised.[146] On a practical level, it has been argued that since tax rules vary across jurisdictions, especially VASPs will be unable to comply due the conflicts that exist between tax rules.[147] The EDPS has also been very dismissive of the inclusion of tax evasion and concluded that processing data for "completely unrelated purpose[s] infringes the data protection principle of purpose limitation and threatens the implementation of the principle of proportionality."[148]

Therefore, strong concerns regarding purpose limitation exist. On the one hand due to the absurdly broad wording of the "original" purposes of countering money laundering and terrorist financing and on the other hand due to the inclusion of another completely unrelated purpose, namely the fight of tax crime. Therefore, the purpose is not specific and the personal data is being processed in incompatible manners.

3.2.2.3 Reporting Obligations

The concerns for reporting obligations build on the previously mentioned criticism of an ever-broadening scope of the AMLD. As obliged entities (arbitrarily) report suspicious transactions to FIUs, which in turn may relay this information to a vast array of public authorities, this may result in the principle of purpose limitation not being adhered to. Sticking to the same example as previously pertaining to taxes, information collected under the AMLD may end up with tax authorities, which may start their own investigations into certain individuals. This clearly violates the principle of purpose limitation.[149] In this way data subjects do not even know which entities hold their data and therefore cannot effectively exercise their rights.[150] The reporting obligations as they currently exist under the AMLD framework therefore frustrate the principle of purpose limitation as the purpose is no longer specified and explicit, and may potentially be further processed in a manner incompatible with the original purpose.

3.2.3 Data Minimisation

The principle of data minimisation builds on the principle of purpose limitation in the sense that data shall be adequate, relevant and limited to what is necessary in relation to the *purposes* for which they are processed (emphasis added).[151] One problem that becomes immediately apparent is the broad formulation of the scope of the AMLD. Since the scope of the AMLD is defined obscenely broad it encourages more data to be processed despite the principle of data minimisation. The broad formulation of the AMLD is therefore inherently critical as it aims to circumvent the principle of data minimisation from the outset, or at least has the result of effectively frustrating the principle of data minimisation. This issue adds to the criticisms mentioned below in relation to the specific compliance duties of obliged entities.

3.2.3.1 Customer Due Diligence

The AMLD does not list exactly which information suffices to fulfil the CDD requirements under Article 13 AMLD, however refers in other parts to information that needs to minimally be held. This is the name, month and year of birth, country of residence and

---

[146] While it may not be explicitly mentioned that tax evasion has been added to the purposes of the AMLD, requiring that information be shared with tax authorities will inevitably have this consequence. See for instance Recital 35; 44 or Article 30(6); 31(4); 49; 50a 5AMLD

[147] On this point see for instance: Mo Egan, 'A Bit(Coin) of a Problem for the EU AML Framework' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

[148] EDPS Opinion 1/2017, paras 29-30

[149] This violation is furthermore aggravated by the obligation of VASPs not to inform data subjects about the transmission or analysis of their data. See Article 39 5AMLD

[150] This issue is covered in Section 3.3, concerned with the rights of data subjects.

[151] Article 5(1)(c) GDPR

nationality.[152] Therefore it can be concluded that this information must also minimally be obtained at the CDD stage. However, given the fact that the AMLD states that "at least" this information needs to be made available, shows that more information may be held. While this would be based on speculation, it may be considered that any additional information held would go beyond the principle of data minimisation for purposes of identifying and verifying a customer's identity. Especially given the fact that some VASPs may additionally hold copies of customers' passports or IDs. Besides this speculative notion, however, there are no concerns pertaining to the principle of data minimisation at the CDD stage.

3.2.3.2 Monitoring

Monitoring results in an additional processing activity and therefore it will have to be considered whether the "ongoing monitoring"[153] required by the AMLD meets the requirements of being adequate, relevant and limited to what is necessary. While it may be argued that occasional checks may allow the VASP to maintain an understanding of its clients and is in its own interest, what matters is to what extent everything is being monitored and if, for instance, copies are being made and retained for longer periods of time. The AMLD mentions that monitoring should be conducted to "ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date".[154] It is thus up to the obliged entities to establish how they do this. To a certain degree at least, since Article 40(1)(b) AMLD requires that evidence of transactions and supporting evidence need to be available for a period of at least five years after the business relationship ends. It therefore *de facto* requires a blanket surveillance system to be in place.

The meticulous noting and recording of every transaction and keeping this on record for years does not adhere to the principle of data minimisation as it fails to distinguish between relevant and non-relevant data and thus is not limited to what is necessary. However, an issue that relates to criminal investigation is that some facts may only reveal their value later. This reasoning may therefore be used to push for a blanket surveillance approach since all data may at some point potentially be relevant. However, such an interpretation would not only fail to respect the ethos of the data minimisation principle, but also assume that every person and every transaction is suspicious regardless of any proven links to serious crime. On top of that, the blanket application of a monitoring obligation frustrates the principle of being innocent until proven guilty and hence endangers the rule of law. It treats any monitoring to be at the same threat-level as that of a criminal investigation, which is simply not the case and furthermore not in line with the AMLD's risk-based approach.[155]

Given the oftentimes delicate nature of matters financed via virtual assets and the fact that many privacy-conscious individuals choose specifically for VASPs since they are not subjected to the same supervision as traditional financial institutions,[156] it must be considered that adding the VASPs to the AMLD framework will strip individuals of the option to choose for more private transactions. Therefore, an approach requiring that as much data as possible is to be retained in

---

[152] Article 30(5) 5AMLD
[153] Article 13(1)(d) 5AMLD
[154] Article 13(1)(d) 5AMLD
[155]The overall departure by the AMLD from a risk-based approach is also highlighted by the EDPS in their Opinion 1/2017, para 50. For a critical assessment of the risk-based approach under the AMLD also see: Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan
[156] Patrick Murck, 'Prepared Statement: Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies' (*Hearing Before the Committee on Homeland Security and Governmental Affairs United States Senate* 18 November 2013) <https://www.govinfo.gov/content/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf> accessed 16 October 2019, 96

case of it being useful at some future point cannot be upheld in liberal democracies that claim to adhere to the rule of law.

While a decisive judgment must be made on a case-by-case basis, the shortcomings discussed thus far (such as the expansive scope of the AMLD, the delicate information revealed particularly via financial transactions and blanket application of surveillance on people with no proven link to a serious crime) suggest that the AMLD, from the outset, fails to adhere to the data minimisation principle regarding the monitoring obligations of obliged entities, as it fosters a culture of blanket surveillance. Furthermore, it fails to demarcate what information would be adequate, relevant and limited to what is necessary and therefore fails to establish a workable regulatory framework.

3.2.3.3 Reporting Obligations

Finally, concerning reporting obligations there are some concerns as well. Obliged entities are required to transfer "all necessary information" to FIUs that may help them with their tasks and additionally need to report even attempted transactions.[157] However, what data is deemed necessary is left to the discretion of the FIU. This level of discretion allows a lot of leeway for FIUs to circumvent the principle of data minimisation.[158]

A second concern refers to the requirement to report attempted transactions. This requirement raises questions whether all requested information will be relevant and adequate if the option seemingly exists to request irrelevant information. Especially in the realm of VASPs it is likely that many attempted transactions fail, and thus remain attempted instead of executed, due to technical and IT issues. Should all such transactions automatically be reported to the FIU? It may thus be suggested that "attempted" should be interpreted to only refer to transactions that were intercepted by the obliged entity unable to identify its customer.[159] Using such an interpretation would address the concern of having to report attempted transactions, however it would also raise questions as to what information about such an attempted transaction would then be shared. If the customer cannot be identified and the transaction did not occur in the end, the attempted transaction arguably does not amount to adequate or relevant information, especially when considering the requirement of treating individuals as innocent until proven guilty.

Therefore, both the fact that an FIU can, seemingly arbitrarily, determine what information it requests from an obliged entity, as well as the fact that attempted transactions must be reported, it can be concluded that the current wording of the AMLD does not adhere to the data minimisation principle as there are no safeguards in place to ensure that data processed is purely adequate, relevant and restricted to necessary information in relation to the purposes of preventing, detecting or combating money laundering and terrorist financing.

3.2.4 Storage Limitation

The fourth principle of data processing regards storage limitation and requires that personal data is "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".[160] Since the purposes of the three main compliance duties differ slightly, these will be discussed in turn below.

---

[157] Article 33(1) 5AMLD

[158] Although Article 35(2)(b) 5AMLD allows obliged entities to deny an FIU request for information where this is clearly disproportionate, this is only permitted in "exceptional circumstances" and does not in and of itself resolve the issue of general disregard for the principle of data minimisation.

[159] Article 14(4) 5AMLD

[160] Article 5(1)(e) 5AMLD

3.2.4.1 Customer Due Diligence

Since the aim of customer due diligence is to identify and verify customers, the identification data relating to customers should be stored only for as long as it is necessary to identify customers. VASPs and other obliged entities have a legitimate interest in being able to identify their customers throughout the duration of their business relationship. However, the AMLD requires obliged entities to retain CDD information for a *minimum* of five years *after* the business relationship has ended, which can be extended by another five years.[161] In cases of long business relationship this wording therefore potentially requires the storage of data for decades.

Instead, a shorter retention period would be more adequate. Five years are a very long time in which it is not really necessary anymore for obliged entities to hold information such as passport scans from former customers. Such a storage period is clearly longer than necessary and therefore fails to adhere to the storage limitation principle.

3.2.4.2 Monitoring

The monitoring obligation is where it gets truly critical. As the ongoing monitoring requires blanket surveillance to be carried out, combining this with retention periods of a minimum of five years after the end of the business relationship results in a gross disregard for the principle of storage limitation.

In *Digital Rights Ireland* the CJEU found that the blanket surveillance of all communication data and the requirement to store it for a minimum of six months was disproportionate. In light of this judgment a retention period of minimally five years *after* the *end* of the business relationship is completely absurd and exceedingly disproportionate, especially if one considers that such a transactions may have occurred decades ago.

While the retention period is based on the belief that some information may become relevant at a later period in time, this brings us back to an argument raised earlier that such an approach may be acceptable concerning surveillance by secret services or of high-risk individuals. However, this line of reasoning cannot be applied in a blanket manner to the entire population without undermining the underlying principles of a *Rechtsstaat*.

Additionally, crimes of money laundering become time-barred at some point and so requiring longer retention of the data seems unjustifiable.[162] Furthermore, as the CJEU clearly pointed out in *Digital Rights Ireland*, the blanket retention of all data is inherently disproportionate and amounts to a serious interference with the fundamental rights to private life and data protection. The Court also criticized that there was no distinction between the data retention periods based on either the person concerned or on objective criteria to ensure that data retention is limited to what is strictly necessary.[163] Following this reasoning, different retention periods could, for instance, apply to persons that are merely suspected, where reasonable grounds exist and finally where the obliged entity knows that a case concerns money laundering or terrorist financing.[164]

---

[161] Article 40(1) 5AMLD; particularly problematic is that no detailed guidelines exist based on which this extension may be implemented, resulting in legal uncertainty and giving rise to serious proportionality concerns, also discussed in Section 4.4.3.

[162] Admittedly, there is quite a difference among Member States regarding time-barring. Regarding the offence of money laundering, for instance, this offence already becomes time-barred after five years in Germany, but only after twelve years in the Netherlands. Perhaps, then, the one-size-fits-all approach of the AMLD offers a political compromise and is, above all, pragmatic and especially suited to VASPs that typically operate across borders. However, this line of argumentation is also flawed. It still does not justify the retention of data for decades during longer business relationships. For the time barring see, for Germany: § 78 (3) Nr. 4 juncto § 261 Strafgesetzbuch (StGB); for the Netherlands: (art. 70, eerste lid, onder 2°, juncto art. 72, tweede lid, Wetboek van Strafrecht (Sr)

[163] *Digital Rights Ireland* paras 63-65

[164] Such an approach would also be in line with WP29 Statement of 1 August 2014 which highlighted the importance of ensuring "that there is no bulk retention of all kinds of data and that, instead, data are subject to appropriate differentiation, limitation or exception". Article 29 Data Protection Working Party, 'Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive ' (14/EN WP 220 adopted 1 August 2014) 2

However, the AMLD fails to distinguish retention periods based on the person concerned or based on other objective criteria to ensure necessity and, in this way, ironically goes against its self-imposed principle of employing a risk-based approach.[165] Considering the case law of the CJEU it must therefore be concluded that the blanket retention of all CDD and transaction data, potentially for decades, is grossly disproportionate and therefore fails to adhere to the principle of storage limitation.

3.2.4.3 Reporting Obligations

Finally, concerning the reporting obligations it is notable that the AMLD argues that the reason why data must be stored excessively long in the first place is because an FIU or competent authority may request this information at an undetermined future moment in order to carry out their duties. As discussed above, however, this does not justify the retention periods of the AMLD. For the rest, the act of reporting itself is not bound to special retention periods, however it is notable that no storage limitation is set for FIUs in the AMLD. This omission therefore also clearly fails to adhere to the principle of storage limitation as no limitation is set to begin with.

In conclusion, the principle of storage limitation is grossly disregarded by the AMLD.

3.2.5 Accuracy, Data Security and Accountability

Finally, there are three more principles to data processing, namely accuracy,[166] data security[167] and accountability.[168] They are more dependent upon specific measures implemented by individual obliged entities and their adherence can better be assessed on a case-by-case basis. Therefore, these principles will not be discussed at this point.

3.2.6 Final Remarks

Having considered the principles of data protection enshrined in the GDPR it becomes apparent that numerous issues exist under the AMLD framework. While some of these are general in nature pertaining to the AMLD as a whole, others apply specifically to VASPs.

The lawfulness of reporting is seriously undermined by a lack of defining 'suspicious' transactions, leaving this to obliged entities to decide. The term itself therefore triggers legal action without adhering to the principle of lawfulness. Furthermore, by defining the aim of the AMLD extremely broad and incorporating other, unrelated, aims, such as tax crime, the principle of purpose limitation is not adhered to at the monitoring and reporting stage. Neither is the principle

---

[165] The overall departure by the AMLD from a risk-based approach is also highlighted by the EDPS in their Opinion 1/2017, para 50. More on the role and development of the risk-based approach in the AMLD: Maria Bergström, 'The Many Uses of Anti-Money Laundering Regulation - Over Time and into the Future' (2018) 19 German Law Journal 1149, 1160

[166] The principle of accuracy entails that the personal data is accurate, and since customer due diligence and regular checks aim to ensure precisely this there is no concern procedurally from the outset from the AMLD generally, or specifically regarding VASPs. Accuracy concerns may arise later through onward transfers of data, for instance if personal data has reached a competent national authority via an FIU and circumstances regarding a customer change. This may not (immediately) be reflected in the data of the authority, however this concern regards databases in general and is in fact a point of common criticism and argumentation to warn about the over-reliance on data(bases). It is however, not a concern specifically regarding to the AMLD framework or VASPs.

[167] The fact that data must be processed in a way to ensure the integrity and confidentiality of the data is dependent upon measures taken by individual obliged entities, in this case VASPs. While VASPs may be more prone to security risks inherent to their virtual activities, it will need to be considered on a case-by-case basis whether the principle of data security is adhered to or not.

[168] The accountability principle may amount to a bureaucratic burden to be borne by the obliged entities, however they were already expected to carry this burden under the GDPR and therefore it does not amount to an additional burden triggered by the implementation of the AMLD or by operating as a VASP.

of data minimisation. Here the broad purpose formulation of the AMLD results in a *de facto* circumvention of the principle of data minimisation from the outset. On top of that FIUs may arbitrarily determine which information they deem necessary and request this from obliged entities. Taken together with the fact that also attempted transactions must be reported, this results in a failure to adhere to the principle of data minimisation at the monitoring and reporting stages. The final general concern refers to the principle of storage limitation at the customer due diligence and monitoring stages. The principle is grossly neglected by outrageous retention periods of minimum five years after the end of the business relationship and on top of that the AMLD fails to distinguish between different data subjects or on the base of other objective criteria.

Regarding VASPs specifically, the lawfulness at the monitoring stage is particularly problematic, considering the oftentimes vulnerable transactions consciously made via VASPs. As such data is quick to amount to special categories of personal data under the GDPR, it is inconceivable that the ongoing monitoring and storing of such information can fulfil the requirements of Article 9 GDPR. Therefore, it must be concluded that the lawfulness principles are not adhered to at the monitoring stage. Neither is the purpose limitation at the monitoring and reporting stage. While generally the principle of purpose limitation is not adhered to due to the broad goal formulations of the AMLD and the inclusion of tax crime, this failure of purpose limitation raises practical issues specifically for VASPs. Due to their virtual nature VASPs will struggle with conflicts in tax rules across jurisdictions, which make it practically impossible for them to comply. These differences in tax rules also amount to different information being relevant in different jurisdictions and therefore further exacerbate the general issue of data minimisation raised.

Together these issues form various serious concerns that amount to the first research question being answered in the negative. It must therefore be concluded that the AMLD measures do not respect the fundamental principles of data processing.

3.3 Data Subject Rights

By now it is clear that the AMLD has a profound impact on the data subject rights of individuals. This section aims to briefly recall which rights have been limited to answer the second research question to what extent the AMLD obligations respect the rights of data subjects. The rights of the data subjects are contained in Chapter III of the GDPR and consist of the right to transparency, which entails the right to information[169] and the right to access,[170] the right to rectification,[171] to erasure,[172] to request the restriction of processing,[173] to data portability,[174] the right to object processing[175] and to not be subject to automated decision making.[176] Additionally data subjects have the right to remedies, which are contained in Chapter VIII.[177]

While these rights are granted in principle, the AMLD already limits the rights available to data subjects from the outset. Being a legal obligation transposed into national law, obliged entities are required to oblige and so the rights to erasure, data portability, to object and to be subjected to automated individual decision-making no longer apply. Additionally, Article 39 of the AMLD prohibits obliged entities to disclose to customers when a money laundering or terrorist financing

[169] Articles 12-14 GDPR
[170] Article 15 GDPR
[171] Article 16 GDPR
[172] Article 17 GDPR
[173] Article 18 GDPR
[174] Article 20 GDPR
[175] Article 21 GDPR
[176] Article 22 GDPR
[177] Articles 77-82 GDPR

analysis is being carried out or when their data is being transferred to an FIU. The prohibition of informing customers, especially of the onward transfer of their data, effectively renders the rights to information, access, rectification and restriction futile as data subjects cannot enforce their rights without knowing who is acting as the controller of the data processing.

The second research question asked to what extent the AMLD obligations respect the rights of data subjects. Considering the aforementioned, a bizarre situation arises where data subjects *de facto* enjoy none of the rights initially enshrined in the GDPR when their data is being passed on to FIUs and national authorities, and in data subjects having seriously restricted rights while their data is still with obliged entities.

IV. Restrictions to Data Subject Rights

4.1 Introduction

While bizarre, in and of itself an extensive restriction of the rights of individuals need not be unlawful. To assess this, the upcoming section will therefore first discuss under which circumstances the rights of data subjects may be restricted within the framework of the GDPR. Since the GDPR gives substance to the fundamental right to data protection enshrined in the Charter,[178] and the grounds of limitation largely overlap,[179] it will simultaneously allow for a judgment to be made whether the AMLD legitimately limits the fundamental rights of individuals. This will, in turn, answer the third and fourth research question.

The GDPR provides, within its framework, that laws may restrict the rights granted to data subjects when three conditions are met. These three conditions are that the restriction must respect the essence of the fundamental rights and freedoms, is a necessary and proportionate measure in a democratic society and aims to safeguard one of ten listed aims.[180]

4.2 Aim of the Restriction

The AMLD brings forward five interrelated reasons to justify the restriction of data subject rights, one of which specifically targets VASPs. This section will dissect these reasons, moving from more general to more specific, to prove that the aims of the AMLD are far from forming a robust foundation for its invasive surveillance practices.[181]

In its recitals the AMLD states that it aims to prevent the use of the financial system for the purposes of money laundering and terrorist financing. In doing so it seeks to protect society from crime and maintain the stability and integrity of the Union's financial system.[182] Thirdly, for data protection purposes, the AMLD claims that the processing of personal data within its realm shall be considered a matter of public interest.[183] In its newest edition, it also mentions the increased security threats of criminal and terrorist groups, stating that preventing the use of the financial system to finance terrorism is an integral part of any strategy addressing this security threat.[184] Fifth and finally, the newest version of the AMLD illuminates that the reason to include some virtual exchanges and custodian wallets to its regime is due to the anonymity that virtual currencies provide and the linked potential misuse.

First of all, it is heavily debated whether these aims are truly met through the AMLD framework. Does criminalising and prosecuting money laundering really protect society from crime? One may argue that if anything, it creates a new crime an in that way actually increases crime statistics. Some also argue that laundering money, the act of bringing illegal proceeds into

[178] Recital 1 GDPR
[179] The grounds on which fundamental rights may be limited under the Charter are listed in Article 52(1) CFR. The limitations must be provided for by law, respect the essence of fundamental rights and freedoms, be necessary and proportional, and finally either pursue an objective of general interest recognized by the European Union or protect the rights and freedoms of others.
[180] Article 23(1) GDPR
[181] This therefore has detrimental implications for the lawfulness of processing, especially but not exclusively, the processing of special categories of data, as discussed in Section 3.2.1.
[182] Recitals 1-2 4AMLD
[183] Article 43 5AMLD
[184] Recital 3 Directive 2018/843

the legitimate economy, does not actually hurt anyone and instead it is more the underlying predicate crimes, such as theft, drug trade and human trafficking, that cause devastation and should be tackled.[185] In fact, this is what most states do in practice.[186] One may counter, of course, that the lack of oversight over a shadow economy comes as a cost to the states, mainly in the form of missed tax revenue. This missed tax revenue is designed to benefit society as a whole (in a social-welfare state), and so the abstract notion of society as a whole is harmed by money laundering. However, this line of argumentation does not quite explain how pursuing money laundering as a criminal offence will reduce (predicate) crimes. Perhaps this reasoning only holds for terrorist financing, where there is a more direct link between the transfer of funds and harm caused to society. It must therefore be concluded that it is neither evident nor supported by evidence that tackling money laundering and terrorist financing reduces crime.

The second argument refers to the protection of the integrity of the financial system.[187] This argument is completely based on assumptions and not backed up by facts.[188] It was the IMF that determined some twenty years ago that crime-money constituted 2-5% of global GDPR, as a 'consensus range'.[189] It is unknown between whom this consensus was found or based on what data it has been constructed. In fact, it has been criticised on numerous accounts, the faulty methodology exposed and the data debunked.[190] However, this criticism has been swiftly ignored by authoritative bodies and by now it has been reiterated so many times that through its pure repetition and endorsement it has become a fact in its own right.[191] This is simply preposterous.

Due to this fact framing and resulting indicative bias,[192] the fight against money laundering and terrorist financing enjoys the status of being a matter of public interest. Initially it formed only a part of the fight on drug trade, however over time it has grown from being a means to being an end in itself. The fight against money laundering has taken on massive regulatory proportions and can truly be called a bureaucratic monster. Cynically one might pose that it creates an abundance of jobs at various levels and by various actors, and after all this is one of the core aims of the European Union.[193] In that sense, it is definitely a public interest. On a more serious note, the

---

185 Carolin Kaiser, 'Privacy and Identity Issues in Financial Transactions - The Proportionality of the European Anti-Money Laundering Legislation' (PhD thesis, University of Groningen 2018) 440; Roberto Lavlle, 'The International Convention for the Suppression of the Financing of Terrorism' (2000) Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 491

186 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

187 It should be noted that this creed stems from a time prior to the credit crisis of 2008, which was unrelated to the presence of crime-money.

188 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

189 Michel Camdessus, 'Money Laundering: the Importance of International Countermeasures' (address at the Plenary Meeting of the Financial Action Task Force on Money Laundering in Paris, 10 February 1998)

190 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality' in Georgios Antonopoulos (ed) *Illegal Entrepreneurship, Organized Crime and Social Control - Studies of Organized Crime* (2016) Springer; Raffaella Barone and Donato Masciandaro, 'Organized Crime, Money Laundering and Legal Economy: Theory and Simulations' (2011) 32(1) European Journal of Law and Economics 115; John Walker and Brigitte Unger, 'Measuring Global Money Laundering: "The Walker Gravity Model"' (2009) 5(2) Review of Law and Economics 821, 823; Friedrich Schneider and Ursula Windischbauer, 'Money Laundering: Some Facts' (2008) 26(4) European Journal of Law and Economics 387

191 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

192 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality' in Georgios Antonopoulos (ed) *Illegal Entrepreneurship, Organized Crime and Social Control - Studies of Organized Crime* (2016) Springer 161

193 Article 3 TEU

struggle surrounding the expansion of the AMLD is more political.[194] As the FATF consists mainly of European Member States it is unsurprising that self-imposed pressure exists to actually implement the measures they preach for the world. Therefore, pulling out at this stage would risk a giant loss of face. This does not mean, however, that the continuous growth of the AMLD should not be challenged. After all the FATF, where these measures originate, is not a democratic body and maintains a minimum level of transparency and accountability to its own operations.[195] It pushes its technocratic agenda internationally through naming and shaming techniques and gains legitimacy through unquestioned adoption into legislation.[196] Therefore, this "public interest" must be challenged as the current system of blind adoption fails to adhere to the rule of law.

The fourth, and related, reason stated by the AMLD is an attempt to justify the restrictions of data subject rights due to the fact that criminal and terrorist groups form an increased threat. Firstly, this wording seems to be an ill-fitted attempt of elevating the importance of money laundering and terror financing to the status of a pressing social need. Perhaps this is in response to the *Tele2 Sverige* judgment where the Court noted that only serious crime is able to justify such serious interferences with fundamental rights.[197] Such an attempt to elevate the level of importance should be viewed critically. In fact, the Article 29 Working Party has stated in the past that the fight against terrorism cannot justify "secret, massive and indiscriminate surveillance programs"[198] and therefore it does not reach the high threshold of "serious crime". Secondly, considering the oftentimes small amounts of funds that are required by terrorists and the fact that they generally do not rely on sophisticated and intricate financial constructions to make ends meet,[199] raises the question to what extent the financial system really plays an *integral* part in their strategies. What is more, terrorists can also raise funds legitimately, for instance through wages earned during their day-jobs.[200] In this way there would, arguably, be no abuse of the financial system. Furthermore, considering that the core business of terrorists may be summarized as causing havoc and destruction, one might more aptly consider that weapons form an *integral* part of their strategies. However, the weapon trade is highly lucrative for several European powers and will therefore not simply be abandoned.[201] While the controversial discussion pertaining to weapon trade is beyond the scope of this thesis, it illustrates that there are potentially more apt places to stop terrorism at the source than through the blanket surveillance of entire populations' financial transactions.

---

194 Carolin Kaiser, 'Privacy and Identity Issues in Financial Transactions - The Proportionality of the European Anti-Money Laundering Legislation' (PhD thesis, University of Groningen 2018) 440; Roberto Lavlle, 'The International Convention for the Suppression of the Financing of Terrorism' (2000) Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 491, 521-523

195 Joshua Cohen and Charles Sabel, 'Global Democracy?' (2004-2005) 37 New York University Journal of International Law and Politics 763, 763-764

196 Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261, 267

197 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016] ECLI:EU:C:2016:970 (*Tele2 Sverige*) para 102 and 115; the argumentation is also in line with that of Case C-311/18 *Schrems II* [2019] Opinion of AG Saugmandsgaard Øe, paras 283-286

198 WP29 Opinion 04/2014, 2

199 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan, 347

200 Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan, 347

201 Selling to Saudi Arabia, which in turn sells to terrorist groups. See for instance: Al Jazeera News, 'Turkey, Saudi Arabia and Europe's 'double standard' in arms sales' (17 October 2019) <https://www.aljazeera.com/news/2019/10/turkey-saudi-arabia-europe-double-standard-arms-sales-191016231548811.html> accessed 4 November 2019; Tom O'Connor, 'How did ISIS get its weapons? Europe wants to limt US and Saudi Arabia Arms sales because guns went to militant group' (*Newsweek*, 14 November 2018) <https://www.newsweek.com/europe-limit-us-saudi-weapons-sales-went-isis-1215758> accessed 4 November 2019

Finally, there is the argument that the anonymity of virtual currencies offers a *potential* for misuse. At this point it may be noticed that a *potential* for misuse will always exist. Therefore, this does not in itself form a convincing argument. In fact, such a reasoning may lead to the uncritical expansion of criminal offences by criminalising increasing amounts of activities, resulting in overcriminalisation.[202] The second view brought forward that virtual currencies offer anonymity is also somewhat flawed. In fact, most virtual currencies must be correctly classified as pseudonymous. Although a user's name and address are not linked to a transaction, his wallet address is.[203] Therefore it will require users to be able to disconnect their transactions entirely from any IP address traceable to them, a rather difficult task.[204] Admittedly, it may require more effort, but through big data and relational analysis it is still quite easy to track down an individual.[205] While this may not be as simple as receiving a name and address, as is the case with financial institutions, the information is still relatively readily available, it simply requires another approach and is certainly not impossible using modern techniques. Therefore, this final argument would also fail to convincingly bring forward a reason as to why hypothetically VASPs should be subjected to the AMLD framework.

For these reasons it must be held that the AMLD framework can hardly be seen as safeguarding the public interests of national security, defence or public security.[206] Considering it is based on estimations at best and absolute fiction at worst it can neither be held to safeguard objectives of general interest.[207] The only public interests that the AMLD truly can pursue is to prevent, detect and prosecute criminal offences.[208] However, this is only so because the AMLD has made money laundering and terrorist financing criminal offences. The circular argumentation quickly becomes apparent. In conclusion it must therefore be held that while the GDPR provides for restrictions of the rights of data subjects in certain circumstances, given the shaky, untrue and outright bizarre foundation on which the AMLD builds, it would be simply illegitimate to grant this regulatory framework the ability to restrict the rights of data subjects under the GDPR.

4.3 The Essence of Fundamental Rights and Freedoms

The second element of Article 23 GDPR requires that the restrictions respect the essence of the fundamental rights and freedoms. For restrictions to fail this requirement they must be so extensive and intrusive so as to devoid the fundamental right of its basic content. Such restrictions can under no circumstances be justified.[209] As was discussed above in Section 3.3, data subjects are *de facto* stripped of almost all of their rights, however CJEU case law may help assess whether the

---

[202] For the concept of overcriminalisation see: Douglas Husak, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press 2008)

[203] Jerry Brito, 'Testimony of Jerry Brito' (Hearing Before the Committee on Homeland Security and Governmental Affairs United States Senate 18 November 2013) <https://www.govinfo.gov/content/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf> accessed 16 October 2019, 35; Christian Rückert, 'Cryptocurrencies and Fundamental Rights' (2019) 5(1) Journal of Cybersecurity, 3

[204] Sesha Kethineni, Ying Cao and Cassandra Dodge, 'Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes (2018) 43 American Journal of Criminal Justice 141, 143

[205] Carolin Kaiser, 'Privacy and Identity Issues in Financial Transactions - The Proportionality of the European Anti-Money Laundering Legislation' (PhD thesis, University of Groningen 2018) 440; Roberto Lavlle, 'The International Convention for the Suppression of the Financing of Terrorism' (2000) Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 491, 525

[206] Article 23(1)(a-c) GDPR

[207] Article 23(1)(e) GDPR

[208] Article 23(1)(d) GDPR

[209] See for instance: European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018) 44; European Data Protection Supervisor, ' Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (2017) (EDPS Necessity Toolkit) 4

extremely high threshold is met of no longer respecting the *essence* of fundamental rights and freedoms.

In the *Schrems* case the CJEU found that the Safe Harbour Decision adversely affected the essence of the fundamental rights to private life and to a legal remedy.[210] This was because public authorities were granted access to the content of electronic communications on a general (non-individual) basis. There was no restriction based on, for instance, the individual or other objective circumstances that may have justified such access. On top of that US legislation did not provide possibilities for non-US residents to pursue legal remedies in order to access, rectify or erase such data.

Similarly, the AMLD provides authorities with blanket access to personal data through the reporting system via obliged entities and FIUs. The access to such data is filtered by two previous institutions and, at least when it originates from the obliged entities, found to be related to a suspicious transaction. Having discussed the problematic notion of the subjective term 'suspicious' in Section 3.2.1.3, it can be argued that nevertheless there is some restriction to the unfettered access to personal data by national authorities. Whether this amounts to an "objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned"[211] remains questionable. Undoubtedly the decision to flag a transaction as 'suspicious' relates to the specific individual concerned, however, as discussed earlier, this classification is neither objective nor does it amount to a proper justification. Furthermore, the AMLD does not come accompanied by "appropriate and verifiable safeguards".[212] In fact, quite the opposite is true. As was also discussed in Section 3.3, by prohibiting the disclosure of investigations or onwards transfers, data subjects are *de facto* stripped of their fundamental rights to data protection. The fact that they may formally still have rights, however cannot enforce these as they do not even know who the controller is in their data processing, does not amount to any type of safeguard. On top of that the arbitrary labelling of 'suspicious' and the blanket nature of surveillance amount to a situation of legal uncertainty devoid of any workable safeguards for individuals. Based on the precedence of *Schrems* the conclusion therefore leans towards the AMLD not respecting the essence of the fundamental rights to private life, data protection and perhaps even legal remedy.

Another case that dealt with the essence of fundamental rights to data protection was *Digital Rights Ireland*. In this case the CJEU held that although the Data Retention Directive seriously interfered with the rights to privacy and personal data protection, the interference did not amount to adversely affect the essence of those rights. This was partly due to the fact that the Directive only required the retention of traffic and location data, but not the actual content of communications. Therefore, it was held that the essence of the fundamental right to private life was not adversely affected.[213] In relation to the fundamental right to data protection it was held that Article 7 of the Data Retention Directive outlined certain data security principles.[214]

In the AMLD a similar article is missing. However, a remnant can be found in the recitals, stating that "specific safeguards be put in place to ensure the security of data and should determine which persons, categories of persons or authorities should have exclusive access to the data retained."[215] On the other hand the monitoring requirements of the AMLD specifically require the content of transactions, as well as any other relevant information, to be retained.[216] On top of that it is also noticeable that obliged entities are required to continue to hold data even though they

[210] CJEU Case C-362/14 *Schrems* [2015] ECLI:EU:C:2015:650 (*Schrems*) paras 94-95
[211] *Schrems* para 34
[212] *Schrems* para 34
[213] *Digital Rights Ireland* para 39
[214] *Digital Rights Ireland* para 40
[215] Recital 44 4AMLD
[216] Article 40 5AMLD

have relayed information to FIUs and authorities.[217] This means that authorities can effectively circumvent their own retention periods as they may always fall back on the databases of obliged entities. The system of the AMLD therefore effectively circumvents data protection safeguards implemented in other regulatory instruments binding national authorities and time-barring the retention of certain data. This is especially true for obliged entities who have customers for decades or even a lifetime. Obliged entities are thus not required to erase data once it is passed on to an FIU or competent authority. Alternatively, no differentiation exists in the retention periods based on the individual involved or other objective criteria. Taken together with the fact that data subjects are *de facto* stripped of their rights once their data is passed on, this situation results in a potentially infinite retention period where data subjects enjoy no rights. Such a situation undeniably affects the essence of the fundamental right to data protection adversely.

Overall, the AMLD may therefore be placed on a spectrum somewhere between the Safe Harbour Decision and the Data Retention Directive. While authorities are granted access to the content of financial transactions, they do not have unfettered blanket access to all transactions. Data subjects are also still entitled to their rights, although they may not actually be able to exercise them, therefore *de facto* stripping them of their rights.

In conclusion, the fundamental rights and freedoms most affected by the AMLD are the rights to privacy, data protection and legal remedy. The expansive monitoring requirements filtered only by the discretion of 'suspicious' transactions do not amount to any substantial safeguards and therefore the essence of the right to private life is at least jeopardised if not compromised entirely. Secondly, despite the AMLD mentioning minimal security safeguards to be implemented at a national level, it must be concluded that potentially infinite retention periods taken together with the *de facto* absence of any safeguards for data subjects, especially in the cases of onwards transfers, results in the essence of the fundamental right to data protection being compromised. Finally, the essence of the fundamental right to legal remedy is not compromised by default, but only in certain situations as the result of non-transparent onward transfers of data. Therefore, taken together, it must be concluded that the AMLD at least adversely affects the essence of the fundamental rights to private life and data protection.

4.4 Appropriateness, Necessity and Proportionality

The final element of Article 23 GDPR requires that any restrictions are necessary and proportionate in a democratic society. Pursuant to settled CJEU case-law, the proportionality of a measure can be assessed only once it is found that a given measure is both appropriate and necessary.[218] Therefore this section will assess each compliance duty to see whether it is appropriate, necessary and proportionate. The section will conclude if and to what extent subjecting VASPs to the AMLD framework would be proportionate.

4.4.1 Appropriateness

For a measure to be deemed appropriate there needs to be a logical link between the measure and the legitimate objective pursued. As discussed in Section 4.2, the only, albeit questionable, aim truly pursued by the AMLD is the prevention, detection and prosecution of criminal offences related to money laundering and terrorist financing. The customer due-diligence (CDD) measures enable the identification and verification of customers and in that way assist potential future prosecution of persons by readily identifying them and in this way connecting illegitimate transfers of funds to these individuals. The monitoring duty *can* facilitate the detection

[217] Article 40 5AMLD
[218] *Digital Rights Ireland* para 46

of potentially illegitimate transactions and in this way may help the AMLD achieve its aim. Finally, the reporting duty allows obliged entities to 'hand over' tasks that lie beyond their scope, such as the prosecution of criminal activities.

By providing information to authorities this duty aids the overall aims of the AMLD, however questionable these may be. In short, it can therefore be said that the customer due-diligence, monitoring and reporting duties that the AMLD imposes may be considered to be appropriate for attaining the objective of preventing, detecting and prosecuting of criminal offences related to money laundering and terrorist financing.

4.4.2 Necessity

Concerning the fundamental right to data protection it must be noted that "any derogations or limitations […] must apply only in so far as is strictly necessary".[219] Furthermore, "in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question."[220]

The CDD measures requiring not only the identification of customers but also their verification can undoubtedly be seen as an effective measure to assist competent authorities with the prosecution of suspects at potential later stages. In its newest wording the AMLD allows for a larger variety of verification methods, now also allowing "any secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities"[221] and in this way may allow less intrusive forms of identification, such as through authorised third-party verification services.

Concerning the monitoring duty of obliged entities, it must be noted that while the blanket surveillance of all transactions may facilitate detection of illegitimate transfers of funds, this duty raises several red flags and is therefore certainly not the least intrusive measure that could be applied. To begin with, monitoring could be based on grounded suspicions or objective criteria that would need to be established. In this way not every person and every transaction would be subject to the invasive monitoring and subsequent storing of their data, potentially for decades. This leads to the next large issue: namely the retention period. A *minimum* of five years *after* the end of the business relationship or occasional transaction will result in gargantuan amounts of transaction data to be collected and stored only because one day it *may* be helpful in a criminal proceeding. For a Directive that argues to aim to fight crime it is remarkable that retention is not based on the threat level of an individual or other crime-related indicator, "it therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[222] It is also not possible to retain the data for a shorter period of time, less than five years. Regarding the data subject rights, it has

---

[219] See for instance: *Tele2 Sverige* para 96; *Schrems* para 92; *Digital Rights Ireland* para 52. Due to the close cooperation between the CJEU and the ECtHR it may also be interesting at this point to mention that, to assess whether a measure is necessary in a democratic society, the ECtHR assesses whether a measure addresses a pressing social need, is proportional and whether the reasons given to justify the interference are relevant and sufficient (see for instance: *S. and Marper v UK* App nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 101). These requirements also broadly resemble those outlined by the Charter (a restriction must be provided for by law, respect the essence of fundamental rights and freedoms, be necessary and proportional, and finally either pursue an objective of general interest recognized by the European Union or protect the rights and freedoms of others) and the GDPR (the restriction must respect the essence of the fundamental rights and freedoms, is a necessary and proportionate measure in a democratic society and aims to safeguard one of ten aims listed in Article 32(1) GDPR). The matters pertaining to a pressing social need are covered in Sections 4.2 and 4.3, proportionality is covered in Section 4.4.3 and the reasons brought forward in Section 4.2.

[220] CJEU Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670 (*Schwarz*) para 46

[221] Article 13(1)(a) 5AMLD

[222] This was a reason for the CJEU to invalidate the Data Retention Directive, see *Digital Rights Ireland* para 58

already been argued earlier that individuals are severely limited and may even *de facto* be stripped entirely of their rights. Furthermore, safeguards pertaining to limits as to who has access to the data as well as other security safeguards are not enshrined in the AMLD, but 'outsourced' via Recital 44 that requires that safeguards must be established at a national level. Together these issues result in a blanket surveillance measure of more or less the entire European population that does not distinguish based on any objective criteria, does not delineate limitations of access, hollows out safeguards for individuals and maintains an obscenely long storage limitation. Such a measure results in a wide-ranging and serious interference with the fundamental rights of individuals and without proper limitations and safeguards may not be deemed to be limited to what is strictly necessary in a democratic society.

Finally, the reporting duty may be seen as effective as it allows for obliged entities to relay potentially decisive information to competent national authorities so that they can carry out their tasks. To the extent that these tasks relate to the prevention, detection and prosecution of criminal offences related to money laundering and terrorist financing it can be concluded that these measures have the potential to be effective. Statistics to this day, however, reveal that this mechanism, while effective, is far from efficient. For example, in 2018 the German FIU received 77,252 reports of suspicious transactions. Only 14,065 resulted in a response by the public prosecutor and a mere 130 resulted in a penalty order.[223] 130 penalty orders amount to negligible 0.92% of public prosecutor responses and a comical 0.17% of initial reports filed that year.[224] This means that the entire AMLD surveillance apparatus and the myriad of people and institutions involved exert incredible effort at the cost of individual fundamental rights and endangering the foundations of our societies for perhaps a few thousand convictions in the entire European Union. Undoubtedly less intrusive measures that would better respect the fundamental rights of individuals would achieve similarly underwhelming figures and therefore it must be concluded that these measures are not necessary within the meaning of the *Schwarz* judgment. Additionally, in the *Tele2 Sverige* judgment the Court stated that "given the seriousness of the interference in the fundamental rights concerned […] only the objective of fighting serious crime is capable of justifying such a measure."[225] As established in Section 4.2, the foundation of money laundering and terrorist financing as crime is shaky, if not outright based on fiction. Such a crime therefore cannot be considered a serious crime equivalent to crimes that truly shake our societies to the core such as warfare, genocide, and more recently acknowledged, environmental crimes.[226] Considering all of this the question naturally arises how it can be deemed necessary that the fundamental rights of millions are curtailed for a few meagre annual convictions of a crime based on thin air and political consensus.

In conclusion it must therefore be found that while generally the CDD duties can be deemed to have some merit, the monitoring and reporting duties raise serious questions as to their necessity. Considering the absolute neglect of safeguards and the fact that less intrusive measures are available, it must be concluded that they do not meet the requirement of being limited to what is strictly necessary in a democratic society.

---

223 Financial Intelligence Unit - Deutschland, 'Jahresbericht 2018' (2018) 18

224 While it might be understandable that not all reports result in a conviction and several reports may be bundled to belong to the same case, it remains baffling that less than 1% of cases brought forward by the public prosecutor resulted in a conviction in 2018.

225 *Tele2 Sverige* para 102

226 This view is shared by the Article 29 Working Party, which states that secret, massive and indiscriminate surveillance programs cannot be justified by the fight against terrorism or other important threats to national security. See WP29 Opinion 04/2014, 2

4.4.3 Proportionality

Having considered the necessity, the final step consists of addressing the proportionality. This is to be done by considering the importance of the objective pursued by the AMLD, the extent of its interference and an assessment of the advantages and disadvantages.[227]

Generally, as discussed previously, the AMLD measures assist potential future prosecution of individuals by readily providing evidence in the form of customer identification and transaction history. The reporting mechanism enables obliged entities to hand over useful information to FIUs and competent authorities, such as tax and law enforcement authorities, to aid with their tasks of preventing, detecting and prosecuting criminal offences. Within the realm of the AMLD these criminal offences relate to money laundering and terrorist financing and specifically aim to prevent and reduce the abuse of the Union's financial system for this.[228] As can be concluded from annual reports of various national FIUs this mechanism is creating an outcome and, in some cases, even leads to convictions.[229] In that sense the AMLD does indeed assist the fight against crime. While this is the major benefit of the AMLD, it additionally creates a variety of jobs within the Union. However, as was also noted throughout this thesis, it does so at the expense of the fundamental rights of individuals, as well as taxpayers, who indirectly finance FIUs and national authorities, and businesses, that are burdened with the costs of compliance.[230, 231]

As discussed in Section 3.2, the AMLD measures fail to adhere to the majority data processing principles. The failure to adhere to the purpose limitation principle is mainly triggered by the broad "original" purpose of the AMLD as well as the inclusion of unrelated purposes such as tax evasion.[232] The major disadvantage of this is that it creates legal uncertainty and simultaneously provides a legal foundation for a blanket surveillance measure.[233] Such a blanket measure is inherently at odds with the AMLD's self-proclaimed risk-based approach.[234] This blanket surveillance measure does not differentiate between data subjects, threat level or other objective criteria and does not require there to be any evidence of a link with serious crime.[235, 236]

---

[227] European Data Protection Supervisor, 'Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (2019) (EDPS Proportionality Guidelines) 13

[228] Recital 1 4AMLD

[229] Joras Ferwerda, 'The Effectiveness of Anti-Money Laundering Policy: A Cost-Benefit Perspective' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

[230] See for instance: Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality' in Georgios Antonopoulos (ed) *Illegal Entrepreneurship, Organized Crime and Social Control - Studies of Organized Crime* (2016) Springer 170ff; Joras Ferwerda, 'The Effectiveness of Anti-Money Laundering Policy: A Cost-Benefit Perspective' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

[231] Concerning the financial burdens an attempt has been made by Ferwerda to allow for a quantitative cost-benefit analysis of the anti-money laundering measures in the Union. Despite a large lack of data being (made) available, his preliminary conclusions indicate that the AMLD measures are highly unlikely to be found proportionate from an economic perspective. Joras Ferwerda, 'The Effectiveness of Anti-Money Laundering Policy: A Cost-Benefit Perspective' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

[232] The disproportionality that arises through this lack of purpose limitation is also discussed in depth in EDPS Opinion 1/2017, para 32

[233] By opting for a blanket measure, a proper proportionality assessment is foregone. See EDPS Opinion 1/2017, para 49

[234] EDPS Opinion 1/2017, para 50

[235] In *Digital Rights Ireland* (paras 58-59) these factors were crucial in the Court's decision to find the Data Retention Directive void.

[236] Reviewing the jurisprudence of the ECHR the Article 29 Working Party has also found that "the proportionality requirement is not met in cases where, among other things, the proposed legislative measure, although fulfilling a legitimate purpose, sets forth a "blanket measure"; fails to assess the effectiveness of existing measures; or fails to provide adequate safeguards for the individual". See EDPS Opinion 1/2017, para 48; Article 29 Data Protection Working Party, 'Opinion 01/2014 on on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (536/14/EN WP 211 adopted 27 February 2014) (WP29 Opinion 01/2014)

Besides the broad scope, the long minimum retention period of the AMLD also disadvantages individuals, as well as the requirement to report all attempted transactions. Particularly problematic is the fact that business relationships, and therefore files kept, may exist for decades, maintaining a shorter retention period is not possible and no objective criteria exist based on which the length of the retention period is to be established.[237] It is known that financial transactions are quick to reveal intimate details about people's lives and therefore, especially in longer business relationships, this combination results in a truly disproportionate mass of delicate data being stored. On top of the disproportionately long retention period concerning obliged entities it is also notable that the AMLD does not include any storage limitations for FIUs. Together with the fact that individuals are not informed when their data is being transferred to an FIU and the fact that data subject rights are substantially curtailed by the AMLD to begin with, the lack of storage limitation can lead to the bizarre situation where data is stored indefinitely and the data subjects have essentially been stripped of their rights.

Given the analyses of the previous sections and the juxtaposition of the advantages and disadvantages in this section, it must be concluded that the AMLD measures in general are not proportionate to the objective they aim to achieve. The failure to adhere to the majority of data processing principles and the outright disregard for data subject rights are not outweighed by the benefits that national FIUs book in the form of a few convictions annually.[238] This is not even considering the shaky foundation on which the entire AMLD framework is built and so serious doubts arise to this surveillance monster as a whole.

On top of general concerns regarding the AMLD framework, several concerns specific to VASPs add to disproportionality of the measures. A major issue relates to the intimate nature of financial transactions and the fact that many users consciously use VASPs to avoid the scrutiny of traditional regulatory schemes.[239] The chilling effect that could result from total surveillance may have substantial impacts on people's private lives and personal development, and in turn shape our societies in rather dystopian ways. Additionally, certain practical issues arise that would particularly, and thus disproportionately, affect VASPs. These issues arise out of the fact that the AMLD uses a state-centric approach while VASPs are inherently virtual and thus exist in several, yet no particular physical locality at any given time. This raises questions where the predicate crime in question is not harmonised at EU level, such as taxes or corruption. Which state's rules apply? To which FIU is a VASP obliged to report to? And what if it is established outside the Union? Despite both the Commission and Parliament wanting to establish harmonised definitions,[240] due to the delay that such a political discussion would cause,[241] it was decided to abandon this effort and instead simply adopt the AMLD where the threshold of serious crimes would apply without

---

237 This, too, was a troublesome point in *Digital Rights Ireland*, paras 63-64.

238 For an attempt to map the costs of compliance with the FATF globally see: Petrus van Duyne, Jackie Harvey and Liliya Gelemerova, 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality' in Georgios Antonopoulos (ed) *Illegal Entrepreneurship, Organized Crime and Social Control - Studies of Organized Crime* (2016) Springer 170ff

239 Patrick Murck, 'Prepared Statement: Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies' (*Hearing Before the Committee on Homeland Security and Governmental Affairs United States Senate* 18 November 2013) <https://www.govinfo.gov/content/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf> accessed 16 October 2019, 95

240 European Commission, 'Commission Staff Working Document: Impact Assessment Accompanying the document: Proposal for a Council Directive implementing enhanced cooperation in the area of financial transaction tax - Analysis of policy options and impacts' (SWD(2013) 28 final 2013), 39; Council of the European Union, ' Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing - Outcome of the European Parliament's first reading' (7387/14 Brussels, 13 March 2014) 11

241 European Commission, 'Commission Staff Working Document: Impact Assessment Accompanying the document: Proposal for a Council Directive implementing enhanced cooperation in the area of financial transaction tax - Analysis of policy options and impacts' (SWD(2013) 28 final 2013), 39

a precise definition existing.[242] Simply outrageous. On top of that, VASPs also include entirely virtual assets and transactions, and it remains highly questionable whether such purely virtual crimes with no real-world consequences should be prosecuted in the real world.[243] However, as long as these questions remain unanswered various important issues remain unresolved for VASPs.

Finally, understanding VASPs and their technologies illuminates that most virtual currencies work with pseudonyms and not anonymously.[244] In most cases individuals can already be readily identified through their meta-data.[245] Additionally, their transactions are automatically logged electronically, for instance in a decentralised log which is the case for cryptocurrencies based on blockchain, a type of virtual asset. On top of that, virtual assets are usually exchanged for fiat currencies or other goods and services 'in the real world' at some point to actually launder the money.[246] At this point one of the vendors or service providers involved is likely to already fall under the AMLD framework.[247] That means that existing technologies and regulations suffice to identify individuals, if necessary. If the aim of the AMLD truly is to fight crime and not to build a complete surveillance state, this objective can already be met with existing tools.

With this the third and fourth research question can also be answered. Considering that most aims pursued by the AMLD are seriously questionable, that the essences of several fundamental rights are compromised and that the measures generally fail to adhere to data protection regulation outlined by the GDPR cannot be found to be in any way proportional, or even necessary in the case of the monitoring duties. For these reasons it must be concluded that the restrictions to the rights of data subjects cannot be justified under the framework of the GDPR. The limitations to the fundamental right to data protection enshrined by the Charter can therefore neither be justified.

---

[242] Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261, 270-271

[243] This was also a central question in the famous US *Ashcroft* judgment, further discussed by Susan Brenner, 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11(1) Vanderbilt Journal of Entertainment and Technology Law 1

[244] Carolin Kaiser, 'Privacy and Identity Issues in Financial Transactions - The Proportionality of the European Anti-Money Laundering Legislation' (PhD thesis, University of Groningen 2018) 339

[245] Christian Rückert, 'Cryptocurrencies and Fundamental Rights' (2019) 5(1) Journal of Cybersecurity, 7; WP 29 Opinion 04/2014, 5

[246] If the virtual assets never enter the "real world" there is no real-world crime, and it remains entirely virtual. For the purposes of this thesis such purely virtual crimes will not be considered. However, discussion exists as to whether such purely virtual currencies should also be subjected to AML regulation. On this matter see for instance: Clare Chambers-Jones, 'Money Laundering in a Virtual World' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan, 165ff

[247] Most likely this will be an exchange provider between fiat and virtual currencies, which have been included in Article 2(1)(g) 5AMLD

V. Conclusion

5.1 Aim of this Thesis

In June 2019 the FATF added VASPs to its framework through the Interpretive Note to Recommendation 15. Since changes in FATF Recommendations have a history of being integrated in updated versions of the AMLD, this thesis set out to analyse, *ex-ante*, the legitimation and justification of subjecting VASPs to the current customer due diligence, monitoring and reporting duties under the AMLD framework. It built on criticisms expressed about the AMLD in general, particularly its disregard for fundamental rights. By combining insights from research in virtual assets as well as research in the proportionality of AML measures, it intended to add a more critical perspective of subjecting VASPs to AML measures. In aiming to achieve this objective, this thesis assessed the AMLD measures of customer due diligence, monitoring and reporting via the framework of the GDPR.

5.2 Findings and Implications

The first research question set out to assess whether the AMLD obligations respect the fundamental principles of processing listed in Article 5 GDPR. During this assessment it became apparent that the combination of essentially arbitrary triggers of surveillance, an ever-broadening purpose definition and ridiculously long retention periods effectively result in a blanket surveillance measure. Very closely related to these concerns are the rights of data subjects. The second research question asked to what extent these rights were being respected. While acknowledging that extremely high threat levels may justify the restriction of data subject rights, under the AMLD it was concluded that the rights of individuals were inadequately curtailed since the proclaimed threat levels were neither high, nor were they supported by evidence.

In chapter four the requirements permitting the restrictions, or limitation, of individuals' rights were assessed in the pursuit of answering the questions whether they were justified. In the assessment of the aims pursued by the AMLD it was highlighted that the foundation upon which the entire system builds is shaky, untrue and outright bizarre. On top of that it was concluded that an overall lack of safeguards for data subjects combined with a practical impossibility to exercise their rights resulted in the essence of at least two fundamental rights to be severely compromised, namely of the rights to data protection and private life. Next, the necessity of the measures was assessed and it was found that the monitoring duties constitute a blanket surveillance measure of more or less the entire European population that does not distinguish based on any objective criteria, does not delineate limitations of access, hollows out safeguards for individuals and maintains an obscenely long storage limitation. The reporting duties raised serious questions due to the lack of effectiveness and whether it can truly be deemed necessary to curtail the rights of millions for a few convictions each year. At this point it was concluded that neither the monitoring nor the reporting duties can be deemed necessary for their objective of fighting money laundering, terrorist financing and tax evasion in a democratic society, especially considering that less intrusive measures could be used instead. Finally, the CJEU does not normally assess proportionality if a measure is deemed not-necessary, however the proportionality of the entirety of the three measures was assessed regardless, as academic exercise. The results were annihilating.

The disadvantages of the AMLD clearly outweigh any (questionable) advantages. While the AMLD may assist prosecution in select cases and create employment, these benefits cannot

be seen to outweigh the structural and blanket surveillance of effectively the entire European population, where individuals have access to limited or no rights and are arbitrarily exposed due to lacking safeguards. On top of these general concerns it was highlighted that VASPs are quick to reveal very intimate details about people's lives, most information is already readily available within existing regulatory frameworks and with existing tools so that the AMLD obligations would be redundant. Finally, the virtual nature of VASPs raises a lot of practical concerns as they operate across European jurisdictions with opposing regulation and the consequences may never transcend to the "real world". Given the faulty foundation that anti-money laundering regulation is based on and its compromising effect on fundamental rights, it was found that subjecting VASPs to the AMLD requirements would not only be redundant and disproportionate, but frankly not necessary. It was therefore concluded that neither the restrictions under the GDPR nor the limitations of the fundamental rights of individuals enshrined in the Charter were justified. The main research question must therefore also be answered negatively: subjecting VASPs to the AMLD customer due diligence, monitoring and reporting requirements is not proportionate. What is more, the monitoring and reporting duties cannot even be found to be necessary in a democratic society and the reporting duties raise serious doubts.

The implications of this assessment emphasised the faultiness of the AMLD framework in general and additionally demonstrated why VASPs particularly, as defined under the FATF, should not be subjected to the AMLD measures. On top of that inferences may also be made about the legitimacy of the AMLD as a whole. While this thesis essentially assessed the GDPR compliance of AMLD measures, these conclusions also have wider implications. The GDPR gives substance to the fundamental right to data protection enshrined in the EU Charter of Fundamental Rights. Therefore, implications about the lack of legitimacy of restrictions to rights granted to data subjects under the GDPR also help illustrate how the AMLD structurally disregards the fundamental rights of individuals enshrined in the Charter. The findings may form part of the consideration taken into account in future amendments of the AMLD or may even form the basis of a claim to be brought in front of the CJEU questioning the legality of the entire AMLD framework. Furthermore, due to their close relationship and concerns already raised in this thesis, the disregard for data protection also has implications for the fundamental right to private life enshrined in both the Charter and the ECHR. Similarly, the cooperation between the two courts means that arguments and lines of reasoning brought forward in this thesis may, where applicable, similarly be used in front of the ECtHR pertaining to the ECHR right to private life.

Finally, given the gross disregard for fundamental rights under the AMLD compliance duties, further explorations into other obligations under the AMLD may be particularly insightful. One such topic was alluded to several times throughout this thesis, namely the issue of onwards transfers of data to FIUs and national authorities.[248] Alternatively, the proportionality of centralised and inter-connected registers may offer another interesting subject of further research.[249]

[248] While not completely unexplored, more research on this would be very insightful. On this topic see for instance: Catherine Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?' (2018) 4(2) European Data Protection Law Review 152; Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261, 289-292

[249] Research is starting to emerge, for instance Arnaud Tailfer and Stéphanie Aféril, 'Register of trusts and privacy: French case law in perspective with the fifth Anti-Money Laundering Directive register' (2018) 24(10) Trusts & Trustees 968 on trust registers and the Master's Thesis by Louise Österberg, 'Anti-Money Laundering and the Right to Privacy: A Study of Potential Conflicts between the Processing of Bank Information to Fight Crime and the Protection of Personal Data' (PhD thesis, Uppsala University 2019) on IBAN registers. The disproportionality of the wide access rights to beneficial ownership registers has also been lamented by the EDPS in its Opinion 1/2017, para 38

5.3 Final Words

A controversial German proverb states that trust is good, but control is better. It seems as though the drafters of the FATF Recommendations and the AMLD have taken this proverb to heart as this regulatory monster seems to grow insatiably, with every edition swallowing up new sectors, employed to execute surveillance work for the states. Under the cloak of security, laws are being passed that would make the drafters of the UDHR turn in their grave. The negative human rights introduced to protect individuals from state interference are swiftly avoided in this way by employing private parties to do the groundwork and offering them a legal basis to pass the gathered information on to government authorities.

As more sophisticated technologies are developed, unprecedented opportunities arise to effectively enforce complete compliance and control. As we reach critical points in the expansion of regulation, it is time to reflect and ask ourselves if we have become a monster ourselves in our fight against crime. With regards to the AMLD, it must sadly be concluded that we have.

Bibliography

Books & Chapters in books

Bergström M, 'The Global AML Regime and the EU AML Directives: Prevention and Control' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

Chambers-Jones C 'Money Laundering in a Virtual World' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

Cohen J, 'Surveillance vs. Privacy: Effects and Implications' in David Gray & Stephen E. Henderson (eds), *Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017)

Egan M, 'A Bit(Coin) of a Problem for the EU AML Framework' in Colin King, Clive Walker, Jimmy Gurulé (eds) T*he Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

European Union Agency for Fundamental Rights, *Handbook on European data protection law - 2018 edition* (Publications Office of the European Union 2018)

Ferwerda J, 'The Effectiveness of Anti-Money Laundering Policy: A Cost-Benefit Perspective' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

Gilmore W, 'Money Laundering: The International Aspect' in Hector MacQueen (ed) *Money Laundering* (Edinburgh University Press 1993)

Husak D, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press 2008)

Nietzsche F, *Also sprach Zarathustra: Ein Buch für Alle und Keinen* (Chemnitz, Germany 1883)

Nietzsche F, *Jenseits von Gut und Böse. Vorspiel einer Philosophie der Zukunft* (Leipzig, Germany 1886)

van Duyne P and Levi M, *Drugs and Money - Managing the Drug Trade and Crime Money in Europe* (Routledge 2005)

van Duyne P, Harvey J and Gelemerova L, 'A 'Risky' Risk Approach: Proportionality in ML/TF Regulation' in Colin King, Clive Walker, Jimmy Gurulé (eds) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (2018) Palgrave Macmillan

van Duyne P, Harvey J and Gelemerova L, 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality' in Georgios Antonopoulos (ed) *Illegal Entrepreneurship, Organized Crime and Social Control - Studies of Organized Crime* (2016) Springer

Van Hoecke M, *Methodologies of Legal Research - Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2013)

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Hachette Book Group 2019)

Journal Articles

Barone R and Masciandaro D, 'Organized Crime, Money Laundering and Legal Economy: Theory and Simulations' (2011) 32(1) European Journal of Law and Economics 115

Bergström M, 'The Many Uses of Anti-Money Laundering Regulation - Over Time and into the Future' (2018) 19 German Law Journal 1149

Brenner B, 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds' (2008) 11(1) Vanderbilt Journal of Entertainment and Technology Law 1

Cohen J and Sabel C, 'Global Democracy?' (2004-2005) 37 New York University Journal of International Law and Politics 763

Jasserand C, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?' (2018) 4(2) European Data Protection Law Review 152

Kethineni S, Cao Y and Dodge C, 'Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes (2018) 43 American Journal of Criminal Justice 141

Koskela H, 'The gaze without eyes: video-surveillance and the changing nature of urban space' (2000) Progress in Human Geography 243

Lavlle R, 'The International Convention for the Suppression of the Financing of Terrorism' (2000) Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 491

Manokha I, 'Surveillance, Panopticism, and Self-Discipline in the Digital Age' (2018) 16(2) Surveillance & Society 219

McCarty-Snead S and Titus Hilby A, 'Research Guide to European Data Protection Law' (University of California, Berkeley School of Law 2013)

Mitsilegas V and Vavoula N, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23(2) Maastricht Journal of European and Comparative Law 261

Rückert C, 'Cryptocurrencies and Fundamental Rights' (2019) 5(1) Journal of Cybersecurity

Schneider F and Windischbauer U, 'Money Laundering: Some Facts' (2008) 26(4) European Journal of Law and Economics 387

Tailfer A and Aféril S, 'Register of trusts and privacy: French case law in perspective with the fifth Anti-Money Laundering Directive register' (2018) 24(10) Trusts & Trustees 968

Vandezande N, 'Virtual currencies under EU anti-money laundering law' 2017 33(3) Computer Law & Security Review 341

Walker J and Unger B, 'Measuring Global Money Laundering: "The Walker Gravity Model"' (2009) 5(2) Review of Law and Economics 821

Zuboff S, 'Big Other: surveillance capitalism and the prospects of an information civilization' (2015) 30 Journal of Information Technology 75

Opinions, Working Papers & Reports

Article 29 Data Protection Working Party, 'Opinion 01/2014 on on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (536/14/EN WP 211 adopted 27 February 2014) (WP29 Opinion 01/2014)

Article 29 Data Protection Working Party, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' (819/14/EN WP 215 adopted 10 April 2014) (WP29 Opinion 04/2014)

Article 29 Data Protection Working Party, 'Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive ' (14/EN WP 220 adopted 1 August 2014)

Case C-311/18 *Schrems II* [2019] Opinion of AG Saugmandsgaard Øe,

Council of the European Union, ' Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing - Outcome of the European Parliament's first reading' (7387/14 Brussels, 13 March 2014)

European Banking Authority, 'Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)' (EBA- Op-2016-07 2016)

European Commission, 'Commission Staff Working Document: Impact Assessment Accompanying the document: Proposal for a Council Directive implementing enhanced cooperation in the area of financial transaction tax - Analysis of policy options and impacts' (SWD(2013) 28 final 2013)

European Data Protection Supervisor, ' Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (2017) (EDPS Necessity Toolkit)

European Data Protection Supervisor, 'Opinion 1/2017 EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications (2017) (EDPS Opinion 1/2017)

European Data Protection Supervisor, 'Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (2019) (EDPS Proportionality Guidelines)

Financial Action Task Force, 'International Standards on Combating Money Laundering and the

Financing of Terrorism & Proliferation - The FATF Recommendations' (Paris, updated June 2019)

United Nations, 'Resolution 68/167: The right to privacy in the digital age' (A/RES/68/167 adopted 18 December 2013)

Websites

Al Jazeera News, 'Turkey, Saudi Arabia and Europe's 'double standard' in arms sales' (17 October 2019) <https://www.aljazeera.com/news/2019/10/turkey-saudi-arabia-europe-double-standard-arms-sales-191016231548811.html> accessed 4 November 2019

European Securities and Markets Authority, 'European Supervisory Framework' <https://www.esma.europa.eu/about-esma/governance/european-supervisory-framework> accessed 1 November 2019

Financial Action Task Force, 'History of the FATF' <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 20 October 2019

Financial Action Task Force, 'Information on updates made to the FATF Recommendations ' <http://www.fatf-gafi.org//publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 20 October 2019

Financial Intelligence Unit - Nederland, 'Meldergroepen' <https://www.fiu-nederland.nl/nl/Meldergroepen> accessed 29 October 2019

Morris C, 'Porn Partnership Pumps This Cryptocurrency Up 22%' (*Fortune*, 17 April 2018) <https://fortune.com/2018/04/17/verge-pornhub-mindgeek-cryptocurrency-brazzers/> accessed 3 November 2019

O'Connor T, 'How did ISIS get its weapons? Europe wants to limt US and Saudi Arabia Arms sales because guns went to militant group' (*Newsweek*, 14 November 2018) <https://www.newsweek.com/europe-limit-us-saudi-weapons-sales-went-isis-1215758> accessed 4 November 2019

United Nations Human Rights Office of the High Commissioner, 'Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Room XXI, Palais des Nations, Geneva' <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E> accessed 23 October 2019

Volt Detschland, 'Unterstütze Volt Deutschland' <https://www.voltdeutschland.org/spenden> accessed 3 November 2019

Other

Brito J, 'Testimony of Jerry Brito' (Hearing Before the Committee on Homeland Security and Governmental Affairs United States Senate 18 November 2013) <https://www.govinfo.gov/content/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf> accessed 16 October 2019

Camdessus M, 'Money Laundering: the Importance of International Countermeasures' (address at the Plenary Meeting of the Financial Action Task Force on Money Laundering in Paris, 10 February 1998)

Financial Intelligence Unit - Deutschland, 'Jahresbericht 2018' (2018)

Kaiser C, 'Privacy and Identity Issues in Financial Transactions - The Proportionality of the European Anti-Money Laundering Legislation' (PhD thesis, University of Groningen 2018)

Murck P, 'Prepared Statement: Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies' (*Hearing Before the Committee on Homeland Security and Governmental Affairs United States Senate* 18 November 2013) <https://www.govinfo.gov/content/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf> accessed 16 October 2019

Österberg L, 'Anti-Money Laundering and the Right to Privacy: A Study of Potential Conflicts between the Processing of Bank Information to Fight Crime and the Protection of Personal Data' (PhD thesis, Uppsala University 2019)