MYKOLAS ROMERIS UNIVERSITY

LAW SCHOOL

INSTITUTE OF PRIVATE LAW

KRISTINA SAUKALIENĖ

LAW, TECHNOLOGY AND BUSINESS

THE CONCEPT OF PRIVACY: LEGAL RESTRICTIONS ON PRIVACY IN THE CONTEXT OF MONEY LAUNDERING PREVENTION

Master thesis

Thesis supervisor:

Doc. Dr. M. Laurinaitis

VILNIUS, 2022

TABLE OF CONTENTS

LIST OF ABBREVIATIONS 3
INTRODUCTION 4
1. PRIVACY 7
1.1. The right to privacy and its boundaries 7
1.2. Personal data in digital era and anonymity in financial transactions 17
2. ANTI-MONEY LAUNDERING 24
2.1. The concept of anti-money laundering 24
2.2. Legislation and AML networking 31
3. JUNCTION OF PRIVACY AND AML 40
3.1 Privacy related AML measures in business-to-client relationship 40
3.2. Privacy exposures in external processing of AML-related personal data 45
4. PROPER IMPLEMENTATION OF PRIVACY RESTRICTIONS IN AML 49
CONCLUSIONS AND RECOMMENDATIONS 56
REFERENCE LIST 58
ABSTRACT 66
SUMMARY 67
HONESTY DECLARATION 68

LIST OF ABBREVIATIONS

1AMLD to 6AMLD – Anti-Money Laundering Directives of respective sequence number

AML – Anti-Money Laundering

ATM – Automated Teller Machine

BTC – Bitcoin (cryptocurrency)

CDD – Customer Due Diligence

CFREU – Charter of Fundamental Rights of the European Union

CJEU – Court of Justice of European Union

ECHR – European Convention on Human Rights

EDPS – the European Data Protection Supervisor

EU – European Union

FATF – Financial Action Task Force

FIU – Financial Intelligence Unit

GDPR – General Data Protection Regulation

GDP – Gross Domestic Product

KYC – Know Your Client

ML – Money Laundering

MONEYVAL – Committee of Experts on the Evaluation of Anti-Money Laundering Measures

ODD – Ongoing Due Diligence

PEP – Politically Exposed Persons

SDD – Simplified Due Diligence

STR – Suspicious Transaction Report

INTRODUCTION

Relevance of the topic and research problem. The scope and imminent raise of illegal activities where unlawful money are generated. Law abiders need to insert this unaccounted income into general circulation of financial funds, this being diametrically opposed to public interest to avoid shaded money and their beneficiaries. Luckily, the society may be protected by proactively gathered information, but this precaution always is unfavorable towards an individual whose personal matters ought to be closely intervened. In every case where two or more contradicting values are collided, the law must set the rules for their prioritization and sacrifices.

This paper analyses the inherent tension between privacy and anti-money laundering regulation where full privacy is uninsurable. The periodical renewals on anti-money laundering legislation, guidelines and tutorials in worldwide jurisdictions emphasizes the global spread of money laundering activities as well as their transformations where law must not follow but to be one step ahead in this battle. Whereas the privacy as one of fundamental human rights is far long recognized and safeguarded, AML regulation is relevantly new. Along its application law faces the challenge to balance different legal interests.

Due to volume of this paper and area of expertise of its author, the analysis of the topic is geographically restricted to EU jurisdiction and home jurisdiction of the author, namely Lithuania. Also the research is focused on relationship in financial sector mainly and broadens to other areas only if needed for analysis purposes.

Scientific research problem and novelty. In the EU, main legislation on protection of personal data is General Data Protection Regulation. It came into force on 25 May 2018, amidst developing AML/CFT framework by already adopted AML4 and upcoming AML5 directives. GDPR recognizes the exemption from general data protection mechanisms in Art. 23, Art. 49 etc., bringing additional questions as to how many personal data should be collected, processed, and stored. But the fundamental dilemma on whether one's right to privacy should at all be restricted by AML, under what conditions and with what safeguards, still lacks exhaustive scientific research. This paper focuses on selected part of this dilemma, namely on identifying correlation points and shaping primary rules for admissible restrictions.

Relevance. The AML framework and GDPR mechanisms are applied for a while, resulting in public awareness, correction of business and personal decisions, even negative consequences in fines for non-compliance with legal rules. Nevertheless, appliance of colliding legal norms often seems to be intuitive, variable respective of jurisdiction or particular case, that results in practitioners uplifting the question on what is and where lies the balance between privacy and AML measures. Undisputedly, legal norms should be examined by legal academics with

scientific methods of analysis employed to ensure compliance with application of other legal norms and coherent judicial decisions in disputes.

Research of the literature. Even though the right to privacy and anti-money laundering as separate concepts are scientifically widely exposed, it must be noted that scientific research level of their cumulative analysis is yet rather low. Insights of practitioners such as Preciosi (2017), Shainski (2019), Parfitt (2019) and Ciesiolka (2019) by their length and research intend to raise awareness of the problem rather than to exhaustively study the topic. On the other hand, some important insights on privacy related puzzles are met in scientific works on adherent legal topics, for example on regulation of electronic money (Laurinaitis, 2015), balancing privacy right and public interests (Lytvinenko, 2017) or privacy in context of information technology development (Pranevičienė, 2011) or national security (Pranevičienė, 2011). Nonetheless, the gap for academics to conduct scientific analysis on privacy in context of AML field is yet to be filled.

The **aim** of the research is to study extensively whether and to what extent a human right to privacy and anti-money laundering rules correlate.

In order to achieve the abovementioned goal, the following **objectives** have been set:

- to reveal the concept of privacy and highlight its evolutions in e-space;
- to analyze money laundering activities in general, focusing on subjects who must be legally supervised in these activities and shaping anti-money laundering concept;
- to disclose points of contact where privacy and AML measures interfere;
- to establish conditions to be met when balancing two legal values, including legal requirements to suppress privacy in AML field.

Statement to defend – a right to privacy can be restricted when anti-money laundering procedures need to be performed.

Practical significance. Due to the abovementioned lack of scientific analysis, this paper shall not only ignite further academic analysis in the field by reviewing the ongoing discussion in academic discourse. The research will also become useful tool for legal practitioners to raise awareness in the topic and avoid unjustifiable harm to any of colliding values.

Research methodology. Seeking to achieve the established aim of the study, various scientific methods were applied complexly. *The systemic analysis method* allowed the author to determine and reflect coherence of legal regulations, to identify their present collisions and evaluate their avoidance alternatives. *The method of semantic analysis* ensured better understanding of the context of terminology, providing maximum certainty in the scope and orientation of the research. The use of *the document's analysis method* revealed the intention of legislators to gain better understanding of the positive law sources used in this research in the

context of related issues. Legislation analyzed in this thesis is in force at the time of preparing of the paper, unless it is explicitly indicated otherwise.

Structure of the thesis. This thesis is structured as follows.

The first part of the paper discloses and details the concept of privacy, emphasizing how in particular this concept has recently emerged due to widespread usage of e-space in almost every field of business and private life of individuals.

The second part reviews the concept of money laundering and, subsequently, anti-money laundering procedures. The researcher identifies policy-making bodies and supervising authorities to disclose the macro-mechanisms of AML network activities.

The third part deals with analysis where and to what extent AML procedures meet right of privacy of subjects identified in previous chapter. An excessive review of *customer due dilligence* principle is made to recognize what personal information is being processed and what legal grounds allow this to be conducted. Also, additional focus is being set on extraterritorial sharing and publishing personal data in AML scope.

Inspired by the observation that right to privacy and AML requirements coincide in so many points of contact, *the fourth part* develops analysis of the conditions for their compatibility. Principles for lawful and justifiable interference into the privacy right in money laundering prevention procedures are investigated. In addition, research is expanded to conditions for proper data processing in AML area. The researcher seeks to maintain the balance to safeguard two contradictory virtues to the best possible extent.

At the end of the thesis conclusions are made and recommendations are offered.

1. PRIVACY

Based on common legal knowledge, privacy rights are vital but not absolute virtues of democratic society. The belief that the one who has nothing to hide, should not be concerned about one's privacy is erroneous both in respect of logic and law. People have legitimate interests in avoiding disclosure about their intimate and personal life: for retaining a full control on how many of and what information they reveal to their surroundings, avoid negative judgements, encounter of biased treatment and even discriminative behavior, etc. Nevertheless, in some cases there are unavoidable collisions of privacy and other law protected virtues, including direct conflicts between privacy rights of several individuals. One of these conflicts is in area of anti-money laundering where provisions protecting society from money laundering activities encompass certain amount of interference into privacy of individuals participating in value exchange relationship. This additional layer of control and prevention to all members of society, applied prior to criminal investigation and legal consequences of the wrongdoers only, creates a hassle among privacy advocates, whose arguments against it range from even slightest disclosure to full autonomy from any inspections. Nevertheless, provisions on justifiable interference on privacy are set by legislation and are to be followed, leaving scholars, practitioners and society to silently reap the benefits of protection or discuss the effectiveness of measures. The research of this thesis joins this discussion with prime focus on two contradicting virtues, a right to privacy first.

1.1. The right to privacy and its boundaries

Legislation. Right to privacy is one of fundamental human rights, referred to in European law also as the *right to respect for private life*. It emerged in international human rights law in the Universal Declaration on Human Rights (1948), as one of the fundamental protected human rights. Based on this document everyone is entitled to enjoy one's privacy, family, home or correspondence undisturbed by arbitrary interference, also honor and reputation without attacks on them (Art. 12).

Soon after adoption of the abovementioned declaration, Europe affirmed this right too in the European Convention of Human Rights (ECHR, 1950). Its article 8 part 1 ensures right for respect for private life, family, home and correspondence. Though succinct, this legislative guarantee is added an extra element, namely the guarantee of undisturbed enjoying the right unless some conditions for interference apply (Art. 8 part 2).

In 2009 the European Union obtained full legal personality and possibility, among others, to sign and adopt international documents. The same year the Charter of Fundamental Rights of

the European Union (2000) came in force with the purpose to promote human rights within the territory of the European Union. The Charter lists right to privacy in Chapter II among 'Freedoms'. The Article 7 guarantees everyone '*a right for respect for his or her private and family life, home and communications*'. Moreover, the Article 8 of the Charter concerns protection of personal data and sets the rule of proper protection by fair processing them for specific purposes on the basis of the consent of the person concerned or some other legitimate basis governed by law. This way Charter enriches human right to privacy with rules for protecting sensitive personal information.

On territorial level, the above listed legislation on privacy colludes by forming two distinct but related mechanisms of protection of fundamental human rights in Europe[1]. First one follows ECHR, though the EU as separate subject is not yet a party to a convention, but all its member states are. All disputes on infringement of human rights under convention are heard in the European Court of Human rights residing in Strasbourg, France. Second system is based on the decisions of the Court of Justice of the European Union (CJEU) which guards due implementation of human rights inside the EU based on principles of the ECHR but mainly following provisions of the Charter of Fundamental Rights of the European Union. Despite both courts are competent to protect right to privacy and right to data protection, analysis of applicable jurisprudence in this thesis is mainly focused on case law of CJEU.

Scope of the right. Right to privacy encompasses enormous areas of persons life, thus it is impossible to list them in legislation. According to the official position of the European Court of Human Rights[2], 'a private life is a broad concept incapable of exhaustive definition. It covers a physical and psychological integrity of a person and may embrace multiple aspects of the persons physical and social identity'. As a result, the scope of definition set in legislation is shaped in every case the European Court of Human Rights hears under article 8 of ECHR. Nonetheless, main protectable ingredients are private life, family life, correspondence and home (Art. 8 part 1 of ECHR). The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases. To note, the concept of 'private life' has been broadly interpreted in the case law, as covering intimate situations, sensitive or confidential information, information that could prejudice the perception of the public against an individual, and even aspects of one's professional life and public behavior. However, the assessment of whether or not there is, or has been, an interference with 'private life' depends on the context and facts of each case.

---

1 Juliane Kokott, Christoph Sobotta. The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR. *International Data Privacy Law*, 2013, Vol. 3, No. 4: 222-223.

2 Guide on Article 8 of the European Convention on Human Rights (updated 31 August 2022): 25, https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

While analyzing human right to live his life privately, which derives from article 8 of European convention on Human rights and is also set in Constitutions of particular member states (i.e., Art. 22 of the Constitution of the Republic of Lithuania), L. Meškauskaitė (2014) notes that this right should be treated as certain autonomy of every person, allowing him or her to be independent from other private subjects and state institutions, in other words, to own a private life under minimum interference of any kind[3]. Though, there must be a proper justification to interfere into one's private life and guard some legal value of higher rank. For example, the Constitution of the Republic of Lithuania[4] allows the interference only based on law and reasoned court decision (Art. 22 part 3). Legal scholars note[5], that for an exceptional activity like interference into private life three criteria must be met: institutionality, legality and reasonableness. On supranational level, the European Convention on Human Rights also lists conditions for public authorities to disturb person's privacy, namely the interference must be performed in accordance with the law, necessary in democratic society in the interests of national security, public safety or economic well-being, crime or disorder prevention, protection of health and morals, protection of rights and freedoms of other people (Art. 8 part 2).

During investigation and comparison of abovementioned legislation it might appear that right to privacy consists only of several elements, namely private and family life, home and correspondence. This conclusion would be faulty, as personal life contains of many aspects and listing all them in laws would be neither possible, nor useful. Thus, legal acts present non exhaustive, but in no way finalized list of privacy dimensions. For example, article 2.23 of the Lithuanian Civil Code gives examples on how right to privacy could be abused: by publishing information about private life without the consent of the person or his heirs, unlawful entrance to private home, surveillance on a person, breach of confidentiality of private mailing or other correspondence, personal notes or information, publishing someone's health related data etc. In jurisprudence of CJEU breach of privacy was found in various situations, i.e., by publishing on a website data with names of beneficiaries of the funds and indicating the amounts received by them[6], taking and storing the fingerprints by national authorities (a severe interference, though justified by protecting against the fraudulent use of passports)[7] or making accessible to any

---

3 Liudvika Meškauskaitė. Asmens teisių apsauga ordinarinėje teisėje: teorija ir neišnaudotos galimybės (The protection of individual rights in ordinary law: theory and missed opportunities). *Asmens teisių gynimas: problemos ir sprendimai (mokslo studija) (The protection of individual rights: problems and solutions (scientific study))*, 355-356. Vilnius: Mykolas Romeris University, 2014. ISBN 978-9955-19-694-5.

4 The Constitution of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=rivwzvpvg&documentId=TAIS.211295&category=TAD.

5 Meškauskaitė, *op. cit*, 356.

6 CJEU, Judgement of 9 November 2010 Volker und Marcus Schecke and Eifert (C-92/09 and C-93/09, EU:C:2010:662).

7 CJEU, Judgement of 17 October 2013, Schwarz (C-291/12, EU:C:2013:670).

member of public the information on beneficial ownership of any entity and legal person established in the country[8]. List of precedents where and how right to privacy was threatened or suppressed is constantly developing in legislation and judicial practice. It should be also mentioned that CJEU and the European Court of Human Rights tend to promote a net restrictive interpretation of the term 'private life' – it should include the protection of personal data being defined as any information relating to any identified or identifiable individual[9].

Right to privacy v. right to protection of personal data. Although these two rights seem interchangeable or at least derived, they are definitely none of that. First, they are enshrined in different articles of CFREU: 'everyone has the right to respect for his or her private and family life, home and communications' (Art. 7) and 'everyone has the right to protection of personal data concerning him or her' (Art. 8). To note, ECHR involves provisions on right to privacy only (Art. 8) and that is probably the result of timeline gap of drafting these two documents (year 2012 v. year 1950), as right to data protection first emerged from Lisbon treaty. Second, the unclear concepts of both analyzed rights are still existing in jurisprudence of CJEU. By analyzing fundamental for private data protection decisions of CJEU in *Digital Rights*[10], *Schrems*[11], *Tele2*[12] and *PNR*[13] cases, Pfisterer (2019) emphasizes[14] that in some of them CJEU treats two rights as independent and separate (*Digital Rights* and *PNR* cases), while other rulings of CJEU lead to the conclusion that the right to the protection of personal data constitutes a fraction of or is secondary to right to privacy or, ultimately, there is an uniform right to privacy which was investigated in respect of processing activities of personal data (*Schrems* and *Tele2* cases). Despite this lack of clarity, it appears rational and reasoned to distinct right to privacy and right to data protection due to their different legislative origins but mostly because of different essence. The great example is unambiguity in subjects of these rights. CJEU acknowledges right to privacy to legal persons under the condition that they identify one or more natural persons in their name (*Schecke* case), i.e., an American law office named 'Sullivan & Cromwell' could, but a local law office name 'Walless' could not. On the other hand, right to protection of personal data is not available to any legal person due to strict subjectivity of personal data holders in legislation. In addition, interference into both rights is treated divergently by CJEU – as compromising the essence of

---

8 CJEU, Judgement of 22 November 2022, WM and Sovim SA (Joined cases C-37/20 and C-601/20, EU:C:2022:912).

9 *Supra note* 1: 223.

10 CJEU, Joined Cases C293/12 & C594/12, Dig. Rts. Ir. v. Minister for Comm., ECLI:EU:C:2014:238, Judgement of 8 Apr. 2014.

11 CJEU, Case C362/14, Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650, Judgement of 6 Oct. 2015.

12 CJEU, Case C-203/15, Tele2 Sverige AB v. Post-och Telestyrelsen, ECLI:EU:C:2016:970, Judgement of 21 Dec. 2016.

13 CJEU, PNR Opinion 1/15, ECLI:EU:C:2017:592, Judgement of 26 July 2017.

14 Valentin M Pfisterer. The right to privacy – a fundamental right in search of its identity: uncovering the CJEU's flawed concept of the right to privacy. *German Law Journal (July 2019)*, Vol 20, Issue 5: 722-733.

fundamental right when right to privacy is considered (*Schrems*) and not yet existing clear analysis on whether any contested measure or procedure has compromised the essence right to data protection[15].

Without doubt, the recent and most comprehensive legislation on privacy protection in Europe is General Data Protection Regulation (GDPR) which entered into force in 2016 and as of 28 May 2018 all subjects were required to comply. This Regulation is applicable directly inside the EU territory for all subjects that process personal data in any way prescribed in GDPR, except exclusions set in the Regulation. In scope of this thesis, exclusions will be analyzed in Chapter 4 of this thesis.

GDPR indicates two levels of personal data that fall under its protection: personal data and special categories data. Namely, the article 4 part 1 identifies, that *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under article 9 of the GDPR as 'special categories' of personal data. The special categories are: (1) personal data revealing racial or ethnic origin, (2) political opinions, (3) religious or philosophical beliefs, (4) trade union membership, (5) genetic data and biometric data processed for the purpose of uniquely identifying a natural person, (6) data concerning health, (7) data concerning a natural person's sex life or sexual orientation. It should also be noted, that processing of these special categories is prohibited, except in limited circumstances set in article 9 of the GDPR.

It is worth mentioning that GDPR covers a very significant list of activities towards personal data. The list includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data[16], including decision making procedures based on automation profiling. Along with the right to due processing of one' s personal data, the data subject is granted additional, secondary rights – right to be informed (about processing of one's data) (Art. 13-14), right to get acquainted

15 *Supra note 14*: 722-733.

16 https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en#:~:text=It%20includes%20the%20collection%2C%20recording,or%20destruction%20of%20personal%20data.

with the data processed (Art. 15), right to request to correct or erase data (Art. 16-17), right to forbid processing of data (Art. 21) and etc.

Under requirements of the EU law, despite GDPR is applicable directly, all member states of the EU made their national legislation compatible with GDPR. In Lithuania certain amendments were made not only to directly data-related legislation, such as the Law on personal data protection, but also to more distinct legal acts like Law on public information.

Scope of right to privacy. After having analyzed the right to privacy and its establishment in main legislation on human rights, it is possible to check whether this right is absolute or, rather, to what extent it is limited when faces other virtues protected by law.

Provision on privacy in the Universal Declaration of Human Rights (1948) is constructed as a prohibition of infringement: *'No one shall be subjected to **arbitrary interference** with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the **right to the protection of the law against such interference** or attacks'* (Art. 12). Although at first sight this appears to be an absolute right, further articles of Declaration set a fair amount of conditions, how any right enshrined in the Declaration, including right to privacy, should be executed duly: to suffer limitations to his rights and freedom only to the extent and solely for the purpose of *'securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society'* (Art. 29 part 2), to be entitled to a *'social and international order'* needed to ensure realization of rights set in the Declaration (Art. 28), also prohibition to exercise one's rights and duties *'contrary to the purposes and principles of the United Nations'* (Art. 29 part 3). Based on this alone, the historic milestone of democratic countries in perspective of protection and execution of human rights is prescribed: the right is acknowledged and protected, but as soon as it threatens to injure particular social virtues of a higher rank (morality, public order and general welfare), the right is restricted or denied.

The European Convention on Human Rights (1950) consolidates the right to privacy with its restrictions in the same provision. Namely, article 8 of ECHR guarantees the right to privacy in its part 1 and sets the 'more important players' protectable at the cost of partial or full interference into privacy: interests of national security, public safety or economic well-being of the countries, crime or disorder prevention, protection of health and morals or protection of rights and freedoms of others. This model is supplemented by additional 'safety nets' of prohibition to abuse rights (Art. 17) and limitation on use of restrictions of rights (Art. 18), where looser or flexible interpretation of restrictions or conditions to apply restrictions to any right set in ECHR is strictly forbidden.

The Charter of Fundamental Rights of the European Union (2000) requires a respect for one's private and family life (Art. 7) but states the condition of executing the right elsewhere. In

addition to certain conditions on how personal data must be duly processed, the Charter develops in article 52, where the scope of guaranteed rights is determined. The latter provisions allow limitation of any human rights set in the Charter only to extent and in situation provided for by law and proportionally. The 'protectable virtues of higher rank' here are the 'objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others'. To note in addition, the scope and interpretation of human rights set in Charter is closely dependent on Convention of Human rights of the European Union, Common Treaties and the Treaty of the EU (Art. 52 parts 2 and 3), so in case of disputed limitation or abuse of right to privacy, provisions in the Charter would be complimentary assisted with the mentioned documents, if needed. Moreover, in the recent case *Ligue des droits humains v Conseil des ministres* on passenger name records (more known in public as 'PNR' case) the CJEU also emphasized, that existence of provisions in Art. 52 of the Chapter is the allowance to lawfully and justifiably interfere into rights and guarantees set in the Charter, including right to privacy (Art. 7) and personal data protection (Art. 8). This finding was used by the court to uphold the Directive on the use of passenger name records on flights between the EU country and any third country for criminal law purposes.

By fulfilling the requirement to consolidate their national legislation with EU laws, member countries transferred provisions on boundaries of the right to privacy into their national laws. For example, Lithuania planted limitations of the right in the Constitution: information on private life can be gathered only if provided by law and on the basis of reasoned court decision (Art. 22). Nevertheless, after joining the EU, Lithuania adapted legal norms of the EU as an integral part of legal system of Lithuania, to the extent of fulfilling the obligations of membership, including contribution to more effective protection of human rights and freedoms[17]. Also, the Civil code of the Republic of Lithuania clearly states that private life is untouchable and any information on private life may be only on basis of consent or a person or his heirs (Art. 2.23). Therefore, it may be concluded, that on every level of legislation in Europe, possibilities to limit or interfere into execution of human rights are prescribed. In order not to transform into unjustifiable interference, these limitations must meet certain criteria of applicability, including an exhaustive list of legal virtues under priority protection.

Challenges for privacy of public persons. It is obvious that one person's right to stay private is contradictory to other person's right to know certain information. If some parts of private life may be valuable to other people merely in scope of pure human curiosity (how much was the cost of the car your neighbor has bought), there are cases where interference into privacy and dissemination of private information is intended to protect real societal interests (your neighbor

[17] The Constitutional act of the republic of Lithuania on the membership of the Republic of Lithuania in the European Union (integral part of the Constitution of the Republic of Lithuania).

participates in criminal organization and transports counterfeit goods with his new car). A right to freedom of opinion and expression (also called freedom of speech) is acknowledged in Art. 19 of UDHR and many subsequent human rights legislation. Generally, it constitutes an undisturbed possibility to communicate one's opinions and share information in any form needed without censorship of government or other society members. Only exclusive reasons lead to restriction of a right of expression, i. e. violation of rights or freedoms of other person or virtues of a society as whole. Based on this right media informs society on matters of public interest, in some ways disclosing private information on someone' s private or family life, correspondence and home. Some scholars[18] note, that essential criteria to contain a balance between right to privacy and right of expression is input of publicly disclosed personal information to a discussion on matter of social importance. Nevertheless, the position of the European Court of Human Rights[19] is unambiguous: 'everyone, including people known to the public, has a legitimate expectation that his or her private life will be protected'.

The same treatment should be applied to personal data that is published, i.e., names and work positions of managers of entities, personal data of public officers or well-known actors, scientists, businessmen, singers or other famous personalities, etc. Neither GDPR, nor previous legislation of personal data protection made any privileges for processing of publicly available personal data, so publicity of personal data does not transform them into non-personal. Public data are not depersonalized, subsequently, gathering and further processing of public personal data does not fall out of scope of GDPR. This leads to conclusion, that all requirements of GDPR are equally applied, including the ones concerning the legal base of data processing and duty to inform the subject about data processing. This concept becomes vital in multiple cases of personal data breaches, i. e. in UK personal data (names, addresses, personal card details, login details, travel booking details) of over 400thou people, the customers and staff of avia company British Airways, were stolen in cyberattack in 2018[20], in Lithuania personal data list of 110thou users (names, phone numbers, e-mail addresses, usernames and passwords) was stolen from a car-sharing company CityBee in 2021[21], etc. In these and other cases criminals have published part or all stolen personal data to persuade public and potential buyers of validity, content and detailedness of data. By placing personal data with free access to certain group / all Internet users, every member of public could see uncovered personal data of victimized data subjects and feel free to perform processing of that data at own disposal not compliant with GDPR requirements. To note, in case the data

18 *Supra note* 3: 358.

19 Guide on Article 8 of the European Convention on Human Rights (updated 31 August 2022). P. 49 / https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

20 https://en.wikipedia.org/wiki/British_Airways_data_breach.

21 https://vdai.lrv.lt/lt/naujienos/automobiliu-nuomos-bendrovei-skirta-bauda-del-duomenu-saugumo-pazeidimo-pagal-bendraji-duomenu-apsaugos-reglamenta.

controller obtained personal data not from data subject, the controller must execute his duty to provide data subject with certain information within a reasonable period after obtaining data but at the latest within one month thereof (Art 14 GDPR). The criminal who performed a data breach, the one who obtained illegally drained personal data or person who saw partial data published on the Web and uses them for processing – none of them probably fears for imposed duties and GDPR related liability (fines) for their unlawful activity, but this does not legitimize the processing of data overall.

Right to be forgotten. When GDPR was enacted, a due protection of personal data also created a new right – the right to object to processing of personal data or in shortened definition, the right to be forgotten. Besides legitimate expectation that one' s personal data will be properly processed; data subject also obtains a right to request data processor to erase these personal data from any mediums of physical and digital form. Notably, for obvious reasons this right is absent in conventional legislation pieces of mid-twentieth century, irrespective to primary provisions on due processing of personal data. While explaining the scope of this right in *Google Spain* case[22], CJEU noted that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed, in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes or in the light of the time that has elapsed.

The right to be forgotten is yet distinct from right to privacy. When *person's* privacy is concerned, it encompasses all information, including not publicly disclosed or known to other person or entity. Whereas right to be forgotten can be implemented only to personal data that were previously exposed to third parties.

Liability for privacy breaches. In general perspective, a liability for violation of a human right, besides circumstances of the particular case, depends on the subject in charge of violation. Whether it is a state (country), governmental or municipal institution, business entity or other person / group of persons, respective of which exactly human right was violated, the victim may be awarded monetary compensation, a public declaration on violation of his/her right, long awaited government decision or, on the contrary, some administrative or legal decision will be annulled. In addition, a piece of national legislation may be amended or declared void if its provisions constitute a breach or unjustified interference to a human right.

More specifically, human right to privacy without presence of undue processing of personal data is protected mainly by respective courts awarding applicants monetary remuneration

[22] CJEU, Judgement of 13 May 2014, Google Spain and Google (C-131/12, EU:C:2014:317).

for disturbance, i.e. payment of pecuniary damages in amount of 6000 Euro and remuneration for costs and expenses in amount of 3000 Euro were awarded for dissemination of private information about the applicant on national television (*Samoylova v. Russia*)[23], remuneration for non-pecuniary damages in amount of 16.000 Euro for each applicant was awarded for mental suffering as a result of prosecutor' s decision to exhumate and re-burry their late husbands who died in a plane crash accident (*Solska and Rybicka v. Poland*)[24], remuneration of pecuniary and non-pecuniary damages in amount of 8.000 Euro and additional remuneration for own costs incurred in judicial process were awarded to son and heir of an applicant for the applicant while alive was denied the benefit of a personal assistant in case of bedridden disability as breach of duty to respect applicant's personal life, deprivation of autonomy and access to the outside world (*Jivan v. Romania*)[25] and many others. All these cases are united by the outcome where – if violation of right to privacy was found – the amount or remuneration is set by the court on the basis of circumstances in particular case heard in court, irrelevant of how much applicant had asked in the claim. There is no highest and lowest brink of amounts when deciding on remuneration, thus the court takes the decision based on the certainty of the judge.

On the contrary, if the right to privacy is violated by undue processing of personal data, the main European guardian of personal data named GDPR offers the ceiling amount for fines. Administrative fines under GDPR are flexible and dependable on size and yearly turnover of the abuser and other circumstances as to durability of the violation, severity of consequences etc., but they vary in range of up to 10mil Euro or up to 2 percent of total worldwide annual turnover for a preceding financial year for entities - in standard cases and in range up to 20mil Euro or up to 4 percent – in severe infringement cases or non-compliance with the order of the supervisory authority (Art. 83 part 5 GDPR). Also, the abovementioned fines are imposed not by courts, but by the EU's data protection authorities and matters are transferred to courts for hearing only if decisions are appealed. If tracked in cumulative registry[26], fines for GDPR breaches vary from several hundred euro to hundreds and millions of euro, though some penalties are not published and the list may not be exhaustive. To date, the biggest fines imposed for non-compliance with GDPR provisions[27] are 746mil euro to Amazon for pushing the unwanted advertisements to users

---

23 The European Court of Human Rights, case Samoylova v. Russia, Application No. 49108/11 / *https://hudoc.echr.coe.int/eng?i=001-213868.*

24 The European Court of Human Rights, case Solska and Rybicka v. Poland, Application Nos. 30491/17 and 31083/17 / *https://hudoc.echr.coe.int/eng?i=001-186135*.

25 The European Court of Human Rights, case Jivan v. Romania, Application No. 62250/19 / https://hudoc.echr.coe.int/eng?i=001-215475.

26 https://www.enforcementtracker.com/,

27 https://termly.io/resources/articles/biggest-gdpr-fines/#:~:text=breaking%20Amazon%20fine.-,1.,for%20Data%20Protection%20(NCDP)., https://www.reuters.com/technology/irish-regulator-fines-facebook-265-mln-euros-over-privacy-breach-2022-11-28/.

in July 2021, 265mil euro to owner of Facebook for insufficient efforts to avoid leak of user's personal data in November 2022, 225mil euro to Whatsapp for multiple breaches and lack of transparency in usage of personal data in 2021, etc. Unlike applicant's remuneration for violation of privacy right, fines for GDPR breaches are not directed to abused data subject but go to governments revenue. Nevertheless, both right to privacy and right to protection of personal data are rather costly to violate.

1.2. Personal data in digital era and anonymity in financial transactions

Recent half of a century saw an enormous leap of development of technologies in almost every area of business and private life. Considering that, the concept of privacy started to broaden and evolute. In 2012 the Human Rights Council of the UN issued a resolution on the promotion, protection and enjoyment of human rights on the Internet during its twentieth regular session in Geneva. In this resolution[28] the Council recognized the open and global nature of the Internet as a driving force in accelerating progress towards development in its various forms and first acknowledged the scope of human rights in physical world same as their scope offline, thus equalizing their protection and promotion. To date, the management of privacy in today's global infrastructure is a complex issue, since it requires the combined application of solutions coming from technology (technical measures), legislation (law and public policy), ethics, and organizational/individual policies and practices.

Scientists allege[29] that the Internet has spawned a massive infrastructure of data brokers that accumulate and track information about individuals. This problem is becoming more and more difficult because of the increased information availability and ease of access as well as the increased computational power provided by today's technology. Thus, the implementing the right to privacy on the Internet brings a new technological aspect of privacy in global network perspective, where people use technologies to give and receive information, including their private data. Scholars[30] distinct three concepts of privacy in this concept:

---

28 Resolution adopted by the Human Council on 16 July 2012 on the Promotion, protection and enjoyment of human rights on the Internet / https://digitallibrary.un.org/record/731540?ln=en.

29 Scott R. Peppet. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, 2014, https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf

30 Valentina Ciriani *et. al*. Theory of privacy and anonymity. University of Milan, 2013: 2, https://www.researchgate.net/profile/Valentina-Ciriani-2/publication/228707386_Theory_of_privacy_and_anonymity/links/545949dd0cf2bccc4912ba17/Theory-of-privacy-and-anonymity.pdf.

- privacy of the *user*, it concerns inability to determine the user in respect of messages he sends, information obtained and actions made in global network. In other words, identities of subjects communicating over global network must be preserved anonymous;
- privacy of the *communication* is protecting the personal information transmitted over the network or by other means of communication, as well as measures to protect content of requests user made to avoid user profiling or even determination of his/her identity;
- privacy of *information* that includes policies, rules and mechanisms to ensure data protection, focusing on a technical measures.

These concepts all are related to privacy, but distinct in their content. It is undisputable, that not all of subjects mentioned before can be acknowledged *human* right to privacy – information and communication, though needed to stay unveiled, are secondary concepts deriving from privacy of a human in global network. Furthermore, despite possibility that a machine is using the global network for some searches, analysis or other actions, machines and robots are not yet granted any subjective rights similar to human ones, therefore further analysis of this thesis section is limited to humanlike origin subjects only. Still, the third one, namely, privacy of *information* is the closest related to anonymity topic.

An important aspect of data protection in the global network implies the protection of identities of the users to whom the particular data may be linked. Subsequently, certain legal and technological measures are taken to guarantee the anonymity of users. As Ciriani (2013) notes[31], anonymity does not fully forbid the release of information, it just demands that the information released is not identifiable. In other words, it protects both: the message and the person messaging by breaking the link between them. Therefore, a particular personal data or set of data made available to third parties still ensures the privacy of data subject while it cannot be used to identify the subject. In general anonymity on the Internet has both benefits (boosts freedom of speech, gives safety to whistleblowers, avoidance of cyber bullying and trolling) and disadvantages (untrue personalities, distortion of published facts, negative effect to life of a person if incorrect facts are published or direct insults are faced on the Internet).

Anonymity in financial transactions. The chosen topic of this thesis determines the money-related context in which the concept of privacy should be investigated. In general, right to private life of a financial asset owner or financial transaction maker should be protected to the extent of minimum disclosure, based on the consent or legislative exclusion. At the same time, the targeted broadest possible level of privacy has downsides – governments who strive to prevent money laundering and financial support to terrorism would lose a valuable tool if financial

[31] *Supra note* 30: 5.

transactions could not be chased. Nowadays most exchanges of valuable things and services take place with participation of money, either in fiat or electronic form, so eternal discussion whether privacy should be enlarged or reduced continues.

When using cash, person can stay anonymous as long as the transaction is lower than amount set in legislation (i.e., in Lithuania the threshold of anonymous cash transactions is 5000 Euro or its equivalent in cash[32], as AML based personality identification rules start to apply from the amount in any form of the money) or the transaction itself is not required to keep a specific legal format (i.e. real estate acquisition always requires approval of a notary[33], so identity check and subsequent ownership registration in a public registry is unavoidable). The challenge lies in the fact that usage of cash is steadily diminishing. In 2019, an exhaustive analysis on usage of cash showed tendency that in almost all analyzed countries cash shares will fall in a period until year 2026 in so much three main stages[34]:

- first, cash and cash checks were first replaced by credit cards with a great level of convenience to use. Also, cash bills of lowest values were replaced by coins in some areas due to longer lifetime of coin in respect of a paper bill (30 years versus 18 months);
- then, paper credit cards were converted into electronic payments (credit transfers) while in Europe paper giro payment orders were shifted to electronic giro payments, allowing to cut costs of maintenance and increase safety;
- subsequently, mobile phone-initiated and Internet-initiated 24/7 payments emerged as immediate transfers of funds with additional convenience in usage and a proper solution for places with a shortage of bank branches or ATMs, especially in less evolved countries. While primary goal of these innovations was to reduce costs and increase convenience, strive for even better effectiveness and cost cutting led to digital cash ideas, i.e., International Monetary Fund suggests creating Central Bank Digital Currency and stay in traditional banking system ensuring access to digital cash through user deposits at a central bank.

With this said, new channels and ways of exchanging value became available and more attractive than carrying and usage of fiat money – rather depreciable paper money and coins in different currencies. It is fair to say that when financial transactions in electronic form are concerned, traditional banking offers some preset degree of privacy by default. To be onboarded as a client to a bank, financial union, electronic money institution or any other financial entity governed and supervised by a government body, a person needs to reveal some personal

---

32 Art. 4 of Law on restrictions of cash payments of the Republic of Lithuania as of 23 June 2022, https://www.infolex.lt/ta/780418.

33 Art. 1.174 of the Civil Code of the Republic of Lithuania.

34 David Humpfrey, Tanai Khiaonarong. Cash use across countries and the demand for Central Bank Digital Currency. IMF Working paper WP/19/46, 2019: 19-22, https://www.imf.org › Files › WPIEA2019046.

information under requirements of KYC rules. Also, when performing payment by using the payment card at vendors or making a banking transaction, the client discloses to his/her home-bank the receiver of the payment, although the purpose of the payment may be left blank or generalized as to 'payment'. While the bank or other financial institution knows and may trace back every transaction in need, there is no anonymity in relationship between the client and the bank and partial anonymity in respect of third persons – global society has no access to information guarded by banking secrecy principle, but it may be disclosed to the court, investigation bodies in cases prescribed by law without even informing the client or generally to any person with previous consent of the client.

Prepaid payment cards are selected payment instrument significant for the research. While traditional debit and credit cards, payment rings, watches and phones are used just as an intermediate material object to pursue a payment with no real cash stored in the object but the object providing a link to the account/information about the account of the owner where funds are kept, prepaid cards work much like a gift card, allowing to spend all the money stored inside the prepaid payment card with neither authentication of the card holder, buyer of the card or person who transferred funds there or any links to the account to debit spendable amount. No presence of bank account linked to the card is needed and the amount spendable from the prepaid card can never exceed the amount inputted there. Also, prepaid cards can be limited in usage variety (in stores of partnering vendors only, no online transactions online using prepaid card number, no cashing out option, works only where Mastercard network reaches[35] etc.) or in top amount stored. The information is given[36], that prepaid payment cards may be restocked in funds via ATMs or any physical location partnering with the card issuer and generally are great alternative to cash. To note, they are more safe, controllable and convenient payment for usage of people with no ability to have an account and use traditional payment cards and in need of reduce risk of carrying fiat money: children, elders, people ineligible for banking services due to temporary or permanent lack of identity documents or official place of residence in the country. Also, they can substitute travel checks for greater safety of the travelling person[37]. Meanwhile, they retain the essential features of fiat money (transportability, interchangeability), are often reloadable and contactless, finally - offer more anonymity than other payment instruments except cash. The risks of terrorism financing based on their anonymity and legislative approach to prepaid cards is further analyzed in subchapter 2.2 of this thesis.

35 https://www.mastercard.co.uk/en-gb/personal/find-a-card/general-prepaid-mastercard.html.
36 https://www.investopedia.com/ask/answers/042315/how-do-prepaid-debit-cards-work.asp.
37 https://ec.europa.eu/newsroom/fisma/items/29693/en.

Cryptocurrencies (Bitcoin, Ethereum and altcoins), on the other hand, are said to offer enormous amount of privacy due to its decentralization and rather flexible legislation. To investigate in more detail on how cryptocurrencies with exchange value provide anonymity for its users, it would be purposeful to take a closer look at their functioning mechanisms.

- *pseudo-anonymous cryptocurrencies (Bitcoin, Ethereum)*. Although it is only pseudo- as will be explained below but not fully anonymous, one of most known crypto coins Bitcoin (BTC) is promoted as a solution to access private transactions. Privacy in Bitcoin system comes from pseudonymous addresses (although fragile and easily compromised), taint analysis, tracking payments and many other mechanisms[38]. Even though, privacy limitations still exist: your privacy stops when you start to spend your money. When a person tries to spend own bitcoins, the transaction goes with inputs (previous owners from whom you received a bitcoin) and outputs (you attach yourself to a recipient of your payment), so a clear ownership chain develops. This way every transaction creates a statistical information that is forever available for analysis. Addresses are linked to real identities at the exchange points when goods and services are obtained (a vendor needs to know whom to ship the product to and governments require exchanges to comply with KYC principles to help combat ML and TF) or when bitcoin is exchanged for fiat currency. Also, there are special tools to track transactions along chains by inputs and outputs. The Ethereum, on the other hand, is constructed not on majority vote for a transaction, but on smart contract basis, nevertheless, they are also trackable if needed and in possession of necessary technical solutions.

- *anonymous cryptocurrencies (Monero, Zerocash)*. Noticeably, some market players resolved particular downsides when introduced improvements to privacy issues and created system very difficult to analyze (ex. Monero uses ring signatures to make links between transactions ambiguous and stealth addresses to break links between transactions and receivers[39]), although there are some ideas on achieving the full privacy. The ultimate private digital currency derived from Zerocash idea, where Zero-knowledge contingent payment (ZKCP) uses zero knowledge proofs to fully mask users and amounts but still ensures that no one is spending their coin twice. According to the co-creator of ZKCP and Bitcoin Core developer Gregory Maxwell[40], their protocol is a complex cryptographic system that allows to prove that specific inputs (transaction) were accepted without revealing anything about those inputs or the operation itself and it was successfully used with Bitcoin currency in 2016. Anyway, besides great level of privacy its

---

38 Gregory Maxwell. Coinjoin: Bitcoin privacy for the real world, august 2013. *Bitcoin Forum*, https://bitcointalk.org/index.php?topic= 279249.0, 2013.

39 Shen Noether. Ring Confidential Transactions / https://eprint.iacr.org/2015/1098.pdf.

40 Gregory Maxwell. The first successful Zero-Knowledge Contingent Payment, https://bitcoincore.org/en/2016/02/26/zero-knowledge-contingent-payments-announcement/.

downsides are low performance by use big amounts of data on working purposes and being sensitive to algorithm faults.

Overall, the high privacy level ensured by Bitcoin and alternative coins could be advocated for using the following valid reasons, most of them applicable to transactions in other forms of money as well:

- ensuring undisturbed business negotiations. If financial information is open to competitors, it may severely downgrade negotiations, facing the increased pressure to admit less beneficial conditions;
- avoiding a predatory pricing. If competitors have knowledge that business is running out of funds, a predatory pricing can be launched to deprive a company of fiat funds completely;
- on a personal level, credit and insurance institutions and even future employers can use information on past transactions against him or her. In example, paying member fee or systematic financial contributions to a political party A might become an obstacle to an employer whose CEO is a heavy sponsor of politician of opposite views, let alone the company itself is in a business relationship with political party B. In addition, belonging to a political party and political views are qualified as special categories data under GDPR to ensure their additional protection;
- long-term durability of data – in further ten years some easily accessible financial information of previous periods can be treated differently by business partners and governments. This way a person may suffer negative consequences for being once engaged in charity organization that later was revealed to participate in illegal activities. Also, into date perspective, trading a cryptocurrencies are often assessed with suspicion so this information could also constitute a hassle in employment procedures if available publicly and public opinion on crypto assets is not changed;
- fungibility of the currency (applied to cryptocurrency mainly). If a certain address is found to be involved in a crime, other users may not accept BTC linked previously to this address somewhere in a chain. In this way that 'greasy' BTC starts to be of different value than BTC without that certain address in a chain.

Based on the assessments above it may be concluded, that despite all odds in modern technical worlds are stacked against them, only fiat money in their cash form may ensure full anonymity in their transactions, provided the amount spent does not fall into identifying and/or reporting duties. Governments are executing control mechanisms over cash flows by setting brinks in amounts of transaction and particular bans on using cash in legal relationship like salary payments, acquisition of real estate etc. As for any mean of electronic money, the highest level of anonymity is given by using prepaid payment cards, though they are in general not applicable in

Lithuania. Cryptocurrencies though, lose their anonymity bonuses on the entrance into and at the exit of cryptocurrency market, when cryptos are bought or sold in traceable manner.

2. ANTI-MONEY LAUNDERING

Having established the concept and boundaries of privacy in area of financial transactions, we are in position to turn scientific attention to the second pillar of the analysis, namely anti-money laundering procedures.

2.1. The concept of anti-money laundering

Definition. Prior to narrowing scientific attention to money laundering and its prevention, a concept of 'money' should be specified. According to scholars, money is historically defined from economic perspective and means anything that can be used to make exchange, has a value or is a value measure, is a payment instrument or a liquid financial asset[41]. As Laurinaitis (2015) explained, money may serve as payment instrument (amount) and a thing (*res corporalis*) - when money seize to participate in relationship as payment instrument, no country uses it in circulation, its value transforms into arising from material thing (numismatic interest)[42]. Either way, criminal activities are producing illegal money as payment means. Money-tangible objects without payment functions are available to be an object of a crime (theft, forgery, etc.), but would never serve as monetary income proceeded to legitimization. In this context, hiding the illicit origins of and further disposal of illegal money is limited to money in their financial capacity.

Though emerged as a way to legalize illicit income from drug trafficking, nowadays money laundering initiatives are spread to basically every segment of illegal activities (human trafficking, drug deals, sale of guns and body organs, prostitution etc.). All of illegal origins need 'washing' out the 'stain' of illegality[43] to avoid negative consequences for their ultimate beneficiaries, same as primarily drug traffickers were concerned of saving their property from forfeiture and themselves from imprisonment. Money laundering in more academic definition is the crime of moving money that has been obtained illegally through financial institutions and businesses to make them seem legally obtained. United Nations convention (Vienna, 1988) defines ML as 'the conversion or transfer of property, knowing that such property is derived from any offence(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offence(s) to evade the legal consequences of his actions' (Art 3.1)[44].

---

41 Marius Laurinaitis, "Elektroninių pinigų teisinis reguliavimas" (doctoral thesis, 2015), 9.

42 *Ibid.*

43 Richard K. Gordon. 'Chapter 15. Anti-Money Laundering Policies – Selected Legal, Political and Economic Issues'. *International Monetary Fund. Current developments in Monetary and Financial Law:* 407, / https://0-www-elibrary-imf-org.library.svsu.edu/view/book/9781557757968/ch15.xml?rskey=32J5Q4&result=14.

44 https://www.unodc.org/unodc/en/money-laundering/overview.html.

Anti-money laundering meanwhile is defined as 'the web of laws and regulations intended to stop criminals from disguising illegally obtained funds as legitimate income'[45], 'controls (that) seek to stop financial criminals from disguising illegally obtained funds as legitimate ones'[46], 'policies, laws and regulations to prevent financial crime'[47], etc. Though no official definition is set in legislation, obviously, the core of definition is AML being rules and procedures to achieve opposite goals that money launderers have and prevent them legitimate their illicit income successfully. The basic idea of AML is to create a coordinated and unified system for prevention and control, whose effectiveness is based on extraterritorial cooperation of various countries, investigation bodies, business entities and society members.

AML rules of identification or verification of clients, monitoring of transaction, filing reports in case of suspicious transactions are applicable to wide range of obliged subjects. First, credit and financial institutions come into the picture. Second, it includes non-bank financial institutions (Electronic money institutions, insurance companies, money exchange entities etc.) that also deal with direct transactions of all type of money and payment instruments. Finally, there are non-financial related business units (casinos, real estate agencies) and business individuals with gatekeeping functions (notaries, accountants, auditors, attorneys, bailiffs). On EU level, the list of obliged subjects was constantly expanding Directive by Directive. It started in 1AMLD by directly pointing at credit and financial institutions and leaving to Member states to discover and specify other obliged professions and entities of non-financial sector, while evolved into broader list with latest additions of cybercrime and environmental offences within 6AMLD. Unfortunately, Lithuanian national legislation does not directly encompass certain units as obliged subjects with respective duties under AML law (part 10 Art 2 of Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania), though their increased vulnerability to participate and be used in AML schemes was pointed out in Lithuanian national evaluation reports (religious organization, charity organizations and other non-profit organizations).

Predicate offences. In AML/CFT related law theory and legislation[48] there is a concept of a predicate offence – the crime that is a component of a more serious crime and generates monetary proceeds. The same breach of law is autonomously punishable under provisions of Criminal code when is conducted with no relation to ML. It may be presumed that every crime that generates income after is finished must be predicate offence to money laundering, but this argument is non sequitur. A standard set of 22 various predicate offences arrived with the passage of 6AMLD, such as underlying criminal activities that generate laundered funds or property

45 https://www.investopedia.com/terms/a/aml.asp.
46 https://www.acams.org/en/resources/aml-glossary-of-terms#a-9799feca.
47 https://sanctionscanner.com/knowledge-base/anti-money-laundering-aml-49.
48 https://aml-cft.net/library/predicate-offence/.

legislated: human trafficking and migrant smuggling, environmental crimes, illegal wildlife trafficking, insider trading and market manipulation, cybercrime, tax crimes on both direct and indirect taxes, fraud, terrorism, forgery etc.

Phases and methods. There is no specific or single-use methodology of money laundering. Instead, a typical ML scheme includes three main phases: *placement, layering and integration/extraction,* but case to case, respective of complexity of activities and amount of illegal proceeds, ML may skip one of abovementioned stages or have one/several of them repeated in more sophisticated schemes.

First, after illegal income is obtained, various methods or combination of them are used to proceed with placement phase, as seen in non-exhaustive list presented above:

- *smurfing*. Large amount of illegal money is divided into smaller transactions and often into different accounts to avoid the requirements of AML/CFT reporting within transactions. In this 'smurfs' or 'deposit experts' are used to create a veneer of independent payers and legality. Besides, often foreign accounts or offshore bank deposits are used to complicate traceability of transactions. As smaller transactions fall below reporting threshold, money is placed into financial system undisturbed;
- *structuring*. Though similar to smurfing, this method does not need additional group of helpers. Money launderers structure funds, that is they break sum into smaller transactions themselves to achieve amounts below the brink of AML/CFT reporting. Interestingly enough, structuring not necessarily includes illegal money – it can be done with someone's legally obtained funds also, but still is a crime as is used to avoid detection by Currency transaction report or even Suspicious transaction report of one's bank[49];
- *aborted transactions*. Similar to perfectly legit business contracts where funds payable are lodged into the escrow account in selected financial institution or into deposit account of a lawyer and returns to the payer if contract is aborted or misconducted, illegal money are lodged with the lawyer or accountant to hold in their client account (depositary account) to settle a proposed transaction or conduct a deal. In short time transaction or deal is aborted and money returned to the client 'money launderer' with a clear and clean purpose[50]. At least in Lithuania this method is limited in use, because the gatekeepers status in respect of AML/CFT was awarded to attorneys, notaries, bailiffs etc. by legislation and range of subjects to open a client's (depository) account in a financial institution is also limited.

[49] https://www.goldinglawyers.com/what-is-smurfing-example-of-how-smurfing-differs-from-structuring/.
[50] https://www.icas.com/professional-resources/anti-money-laundering-resources/latest-developments/aml-awareness-three-stages-of-money-laundering.

- *using shell companies and trusts*. These entities exist only on paper and do not perform any real business activity (other than intended for money laundering purposes) or own any tangible and intangible assets. Existence of such companies is legally neutral, although they become illegal when used for illegitimate purposes as money laundering, tax evasion and tax avoidance[51]. Fictitious companies can be used in sale relationship, performing of fictitious transactions, to hide the ultimate beneficiary, to expand the chain of transactions or sales, to pretend the funds in question are obtained legally from a shell company for some non-existing services or not sold goods, etc. In addition to no business activities, the banking operations of these shell entities are not economically rational, no physical team exists at their office address and often they are registered in hardly adjusted places for business or many entities in one address. In year 2018 media investigation was made in the capital of Lithuania on five addresses with the biggest number of hosted entities – top leaders were a small apartment owned by the old lady, nonresidential premises in suburb, even a mystical room with number not existing in old business building, but also a company providing services of virtual business address and processing correspondence[52]. In addition, owners of these shell entities are also disguised as their real addresses differ from those presented to the registries;
- *using cash-intensive business*. Here cash obtained from illegal activity is merged by addition to legal income from a cover cash-friendly business. It might look like a 'renaissance' of first money laundering offices where legit laundering services were provided, but nowadays more sophisticated businesses are involved – gambling, hairdressers and barbers offices, virtual gaming, casinos etc.

Second, after successfully placed into the financial system, illegal proceeds need to be layered to hide their origins and destruct traceability of operations along with avoiding reporting and identification procedures performed by financial institutions. Through wire transfers dirty money spread or travel through various financial institutions, most often crossing different jurisdictions.

Finally, the time to reap the fruits comes. In integration or extraction stage illicit funds are used to obtain luxury goods or long-term valuable things (jewelry and watches, real estate, pleasure yachts etc.) or extract in their monetary form by means of issuing fake loans that never will be returned, paying dividends to criminals from elevated empty profit or using fake employees to pay them official salary and later recollect it in cash[53]. It may be presumed, that soon after

51 https://www.tookitaki.com/compliance_hub/shell-companies-money-laundering/.

52 https://www.15min.lt/verslas/naujiena/finansai/penkiais-adresai-iregistruota-7000-imoniu-15min-aplanke-ir-atradimai-sokiravo-662-1025250.

53 https://www.icas.com/professional-resources/anti-money-laundering-resources/latest-developments/aml-awareness-three-stages-of-money-laundering.

extracting funds in cash they are employed by purchasing some tangible goods or intangible property or penetrated back into business, as storing big amounts of money in fiat is rather place consuming and sensitive to physical destruction or devaluation. Anyway, integrated funds do not create explanation of their receival so range of obtainable goods is limited by excluding those adjacent to personal identification and proving origin of funds.

Every year app. 1,6 trillion USD of illicit funds are laundered around the globe and despite artificial intelligence and AML mechanisms employed, only 1 percent of illegal income is seized and frozen[54]. According to United Nation Office on Drugs and Crime, the estimated yearly amount of globally laundered money is 2-5 percent of global GDP (800 billion – 2 trillion USD in their current value)[55]. Besides, ML has huge impact on the society not only in direct occurrence where some people become richer by illicit origins. ML activities allow corruption to prosper, lead to social degeneration. It shakes the economic system and increases country reputation risk that leads to lower rankings in international financial markets and lower attraction to investments, resulting in decrease of GDP of that country. Ultimately, ML boosts criminal activity rates in the country and region, decreasing stability and trust in the society thereof.

Money laundering in cryptocurrency. As money launderers evolve following transformation of payment methods and means, a separate area for illicit activities exists. Nevertheless, the same rules and stages that apply to ML in cash also transfer to ML activities using cryptocurrency[56]. In placement stage**,** cryptocurrency is inserted into the system, either as received income for illicit business (human trafficking, drugs or guns sale, etc.) or purchased for fiat money of illegal origins. Layering stage is generally not needed or at least non exhaustive – cryptocurrencies operate on a concept of anonymity, so traceability of transactions is not needed after placement stage. Despite that additional efforts are often made to break links between transactions detectable by following back the blockchain. Last, integration phase is conducted in two steps. As criminal is possessing placed and layered cryptocurrency, to use it for acquisition of luxury things it is necessary to transform crypto into fiat/electronic money and cryptocurrency exchange entities are needed. Although AML/CFT regulation is expanded to cryptocurrency exchanges as well, flexible or negligent subjects can give a helping hand. Otherwise, the criminal may obtain needed valuable things from vendors who accept payments in cryptocurrency. Ultimately, explanation phase of value of cryptocurrency in possession is easier than in cases with

54 Rina Shainski. For Banks, Data Privacy and Anti-Money Laundering Don't Have to Be Incompatible (2019), https://www.cpomagazine.com/data-privacy/for-banks-data-privacy-and-anti-money-laundering-dont-have-to-be-incompatible/.

55 https://www.unodc.org/unodc/en/money-laundering/overview.html.

56 https://financialcrimeacademy.org/money-laundering-cryptocurrency/.

fiat money because decentralized market of cryptocurrency assets often has no solid value basis, therefore their value is very versatile over a short period of time.

Reverse ML. In traditional money laundering scheme, initially illicit funds emerge and further activities are aimed to clean (legalize) them. On the other hand, the opposing mechanism exists, where totally legal money are directed in to use in criminal activity in restricted to society ways so that money gets illicit in their ultimate destination of use. So the process of conducting financial transactions with legit money to conceal or disguise their future use for criminal purposes is called reverse ML.

Criminals of various 'illegal specialization' are using clean money to commit their crimes in future. Probably the greatest example of this is a terrorist financing where legal proceeds are collected via charities, business organizations and other intermediaries and used for illegal purposes. The deadly attacks in the USA of 11 September 2001 are investigated[57] to have been financed with cash and money transfers from abroad – some funds originated from money exchange in the United Arab Emirates and travelled through the correspondent bank in New York, USA towards hijackers of deadly planes in their bank in Florida, USA, also bundles of cash were smuggled into the USA by hijackers and their helpers. In their starting points all these funds may have been perfectly legitimate but at the end of their voyage they dropped below the line of legality. As Casella S. D. notes[58], if the focus on these purely legit money will stay on their origins, the fatal consequences in their usage will not be prevented – it is the manner in which money are moved that is the clue to the intended future non-law-abiding use.

Liability for ML and predicate offences. It must be noted that any predicate offence from the 'list' in its essence is an autonomous illegal act that provisioned in criminal code and punishable based on legislation in the destination country. But when it is an integral part of other criminal activity (i.e., AML), the dilemma on bases for sanctioning of predicate offender emerges.

First, the liability grounds for ML should be investigated. There are no provisions in any of six AMLDs on criminal sanctions for ML or composition of the crime, these must be set by Member states. Therefore, in Lithuania, for instance, criminal liability for ML is found in two articles of Criminal code of the Republic of Lithuania: article 189 'Acquisition or sale of the property obtained through crime' and article 216 'Legalization of criminally obtained property'. Both articles were amended in year 2021 to comply with AMLDs and MONEYVAL recommendations to Lithuania on due transfer of AMLDs provisions into national legislation and effective implementation of AML measures. The person can be punished under article 189 if

---

57 Stefan D. Cassella. Reverse money laundering. *Journal of Money laundering control*. London, Vol. 7 (1), Summer 2003: 92, https://www.proquest.com/docview/235831715.

58 *Ibid*.

he/she knowingly acquired, managed, used or realized the property obtained through or from a crime. Sanctions vary from public works, fine or arrest for property of small value to restriction of liberty, arrest or deprivation of liberty for up to six years, if the crime was committed in respect of a property of high value or great historical, cultural or scientific significance. Legal person may also be sanctioned based on provisions of this article, except actions in regard of small value property. Whereas liability emerges from article 216 for natural or legal person, who legalized or ordered to legalize own or another person's property or assisted to other person to avoid consequences of this act or made other listed actions with knowingly illegal property. Again, sanction comes in range from a fine to imprisonment for up to seven years. The distinction between the abovesaid two articles of a Criminal code lie in stage of the ML process where legal liability is applied. Article 189 is supposedly aimed at final integration stage, while article 216 may be used more flexibly during other ML stages. Notably, both articles have in common the compulsory element of actions performed knowingly, being aware of illegal origins of the property. Therefore, no criminal liability can be imposed on a participant of ML scheme, including money mule, when no evidence of him or her being sufficiently aware of illegal origins of the property (funds or other types of property) exist. Those misinformed or unaware money mules[59] or other one-off participants to ML might lose their money (owned or promised as payment for assistance), face a criminal investigation, be deprived of compromised bank account and probably left with future note on unwanted financial relationship in that financial institution, may have lower credit records, temporary arrest on their property for the period of investigation, etc.

To note, AML related legislation of EU level also has no provisions on whether *the predicate offender* should face a separate legal liability and punishment for participation in ML, the question of their liability is similarly left for disposal of Member states of the EU. On the former example of Lithuanian legislation, it may be concluded, that unless the predicate offender also performs actions that fall within the scope of articles 189 and/or 216 of the Criminal code, the predicate offender faces legal liability based on particular provision of criminal law where his predicate offence is criminalized.

As it happens, tax related crimes (evasion or avoidance) are often adjacent to ML schemes due to criminal's aim at not only clean the money for further use, but also avoid additional financial losses in a form of payables to the state. The composition of criminal provisions do not include actions in scope of tax, so in often investigation and criminal case, additional grounds for legal liability of money launderer would arise from the Criminal code (providing false information about

[59] Money mules - people who receive and further transfer funds to criminals or allow criminals to use their bank account for transfers of illegal money while being paid for assistance.

income, profits or assets (Art. 220), fraudulent or negligent financial accounting (Art. 222-223), etc.).

2.2. Legislation and AML networking

Since mid-1980s, all developed countries and great number of developing ones have enacted legislation to criminalize money laundering activities[60]. As this analysis is limited geographically to the European Union territory, the unwrapping of AML related legal framework on the EU level will continue with emphasizes on main developments thereof.

The history is being traced back to year 1991 when Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (1AMLD) was enacted. At the time European Community was two more years until transformed into the European Union and separate countries made efforts to combat ML in uncoordinated ways, although worldwide initiatives on strengthening AML policies in year 1989 led to establishment of FATF by G-7 Summit in Paris. FATF is an inter-governmental body to set international standards on combatting AML/CFT or, as they are portraying themselves, a 'global money laundering and terrorist financing watchdog'[61]. 1AMLD emphasized the significance of supplementing national level measures of AML in particular Member states with international coordination and cooperation to be able to international context of disguising the criminal origin of the funds and generally strengthened the role of the Commission and its adjacent legislation pieces. 1AMLD clarified the definition of ML, forbid it as the activity and required member states to criminalize money laundering activities (Art 2 of 1AMLD). It should be noted that in preamble of the directive it was acknowledged that ML is conducted not only via credit and financial institutions but 1AMLD imposed additional duties for the latter subjects particularly, whereas other types of professions and categories of undertakings whose activities are particularly likely to be used for ML purposes were left to be identified and included into AML measures by Member states themselves.

It took next ten years to renew AML legislation on the EU level. Shortly after establishment of the body, in year 1990 FATF issued a report containing a set of Forty Recommendations, aimed at provision of comprehensive plan of action needed to fight ML[62]. FATF also called all countries to enable them by inserting into or adjusting the existing national legal frameworks. Due to evolution in legal relationships and economy, as well as criminal world, in a decade since 1AMLD more clarity appeared as to what other subjects besides credit and

60 *Supra note* 57.
61 https://www.fatf-gafi.org/about/.
62 https://www.fatf-gafi.org/about/historyofthefatf/.

financial institutions are riskier in scope of ML, what activities present more likeness to be involved in ML, whom and how to report if any suspicious is noticed etc. Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering[63] (2AMLD) expands list of subjects vulnerable to participate in ML and to whom obligations laid down in a directive are imposed by including players of non-financial business: auditors, accountants, tax advisors, real estate agents, casinos, dealers in high-value goods whenever payment was made in cash exceeding 15thou euro, notaries and other independent legal professionals if they assist their clients or perform on behalf of the client certain activities listed in a directive (Art 2 of 2AMLD).

Next leap towards improvement of legislation was made in year 2005. Fatal outcome of hijacking events on 11 September 2001 in the USA showed urgent need for new provisions on prevention of and combatting terrorism financing. The mentioned terrorism events led to review and renewal of FATF recommendations and 9 new recommendations in respect of terrorism financing were added to the package. Main principles of the latter were mirrored in Directive 2006/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[64] (3AMLD). The directive was not, however, revolutionary, it rather went beyond larger extent than previous directives. Perhaps two most significant changes besides CTF provisions were i) extending the list of persons that are subject to directive – trust and company service providers were included, and ii) introducing risk-based approach to AML procedures that allowed to classify clients respective of their credit portfolio, type of business activities etc. and adjust the 'depth' of performed CDD accordingly. Moreover, provisions of the directive are applicable to actions also performed on the Internet (part 14 of preamble of 3AMLD).

It took a decade again for upgraded Directive on AML to appear, though possibilities for money launderers to use fast-developing payment related technologies and cross-border data flows extended far beyond the regulative framework. Directive 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[65] (4AMLD) was enacted. The Directive had to be transferred into national legislation of Members states until year 2017. It

63 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001L0097&from=EN.
64 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0060&from=EN.
65 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

aligned the EU legislation in AML area with latest FATF recommendations and further expanded list of obliged subjects: casinos from 3AMLD were joined by other fellow units in 'gambling business', also designated non-financial business and professions list was supplemented by other persons trading in goods in inflow or outflow of payments or cash exceeding 10thou euro, irrespective if one or more linked operations were performed (Art. 2 of 4AMLD). In essence, by setting a brink of 10thou euro for occasional (out of business transactions) and 1thou euro for transfer of funds (Art. 11 of 4AMLD) where obliged subjects must perform CDD and transaction monitoring schemes, 4AMLD broadened not only the list of subjects obliged with duties, but also of subjects under supervision. Moreover, 4AMLD gave birth to obligatory including UBOs into national registries to strengthen transparency of entities and formations these UBOs benefit from (part 14 of preamble of 4AMLD).

Promptly after implementation of 4AMLD the EU introduced the next one. Directive 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[66] (5AMLD) made some significant developments towards effective AML and CTF, in particular[67]:

- expanded list of obliged subjects by inserting virtual currency exchanges and custodian wallets, also developed definitions of several other list members: accountants, art traders, estate agents etc. (Art. 2 of 5AMLD). In 5AMLD a cryptocurrency sector was first included into scope of AML regulation on European level;

- made registries of beneficial owners of legal entities open to public. Data on beneficial owners of trusts are made open to FIUs, obliged subjects in financial system, also third persons under legitimate interest. National registries on beneficial ownership will be interconnected directly for boost of cooperation in AML field. Also, Member states will have to set up centralized bank account registries to ensure identification of bank accounts' owners;

- reduced anonymity brink of general-purpose prepaid cards, allowing them to be anonymously used in shops within 150 euro limit and online if transaction amounts within 50 euro. Also, Member states are allowed in national legislation to decide whether general purposes prepaid cards should be forbidden inside their territory. The Directive emphasizes that prepaid cards are legit and contribute to financial developments, nonetheless they are anonymous and thus easy to use for terrorism aims. Investigators officially announced to have discovered that series of terrorism-shaped attacks in Paris, that took place in November 2015 and were coordinated by

66 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN.

67 Directorate General for Justice and Consumers of the Commission. Strengthened EU rules to prevent money laundering and terrorism financing (Fact sheet) 9 July 2018, https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=48935.

Islamist terrorists, where 130 people were killed and 416 were injured, have been funded via prepaid cards[68], so additional measures as compulsory checks of identities, lowered thresholds of amounts used by prepaid cards were aimed at reduction of opportunities of terrorist formations to perform;

- enhancing the powers of FIUs in Member states and their access to vital information via central bank, registries and data recovery systems.

On 20 July 2021 the European Commission has announced an extensive set of legislative proposals intended to strengthen AML/CFT rules (so called the 'AML Action plan') and the new legislative framework should be fully operational in year 2024. Among novelties, the Authority for AML/CFT (AMLA) is being established, proposals of Regulation on prevention of the use of the financial system for the purposes of ML/TF and Regulation on information accompanying transfers of funds and certain crypto-assets were introduced and next AMLD was adopted. On the latter, the Directive of the European Parliament and Council of 20 July 2021 on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849[69] (6AMLD) came into effect with an implementation deadline for financial institutions in Member states set within one year. This legislative piece reverted the attention to the root concepts of AML in respect of how methods and schemes of money launderers evolved, aiming at unifying the definition and understanding of money laundering on the European Union level.

Furthermore, assistance abetting, inciting and attempts to commit a money laundering activity was acknowledged money laundering itself and criminalized respectively. With this development liability is extended to various associates (knowingly) aiding to money launderers. Even more, legal persons (companies and other formations) were included into scope as prosecution and potential liability subjects, being not only direct beneficiaries in money laundering, but – so to say – negligent position to ML activities inside the company. Penalization changes include increase of minimum prison sentence term from 1 year to 4 years, and any sentence can be joined by fine in amount up to 5mil euro. This was needed to ensure consistency in punishments across Member states and necessity to apply adequate penalties at least in percentages of amounts of funds laundered.

More sophisticated development in 6AMLD is a list of 22 predicate offences for money laundering to be criminalized, including cybercrime and environmental violations among them.

---

68 https://ec.europa.eu/newsroom/fisma/items/29693/en; https://en.wikipedia.org/wiki/November_2015_Paris_attacks.

69 Directive of the European Parliament and Council of 20 July 2021 on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0423&from=EN/.

Member states were obliged to make sure these law offences are not only properly criminalized in national legislation, but also recognizable as a part of AML schemes during inspection of client's activities and duly investigated. Finally, 6AMLD encouraged and boosted the cooperation between Member states in prosecution of ML crimes. Investigations and prosecution of offenders should become borderless. Due to its rather short term of validity, 6AMLD is yet short of deficiencies and criticism. At this point it is not clear whether and for how long this Directive will survive the test of effectiveness.

Local legislation. The EU provisions are the source of national implementing provisions and if there is ever any conflict regarding the applicable provisions, the EU legislation prevails. However, domestic laws may go further than the minimum standards set in directives. Meanwhile, in addition to AMLDs, Member states of the EU have national legislation where they may provide even more detailed, as long as not contradictory rules to implement AML aims and requirements (i.e., as set in Art. 5 3AMLD, etc.).

In Lithuania main piece of AML on national level is Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania[70]. It may be concluded that this document keeps pace with developments on the EU level – the latest amendment to this law entered into force on 1 November 2022 and included virtual currency exchange and e-wallet service providers in the list of subjects obliged to comply with AML requirements: customer identification and verification, transaction monitoring, reporting and information provision under request of authorities etc. Also, the mentioned subjects were obliged to employ AML reporting officer that is allowed to work only in one entity providing cryptocurrency services, have their senior officers of management and supervision functions with impeccable reputation, place of permanent residence of senior CEO must be in Lithuania etc. Newest amendment to this law also provide some AML related obligations to ICO offerors.

In addition, the regulation is also set in documents of lower rank, mainly issued by competent supervision bodies. The Financial Crime Investigation Service is the body responsible for protecting the state financial system by disclosing violations of law, including implementation of money laundering and terrorist financing prevention measures, conducts pre-trial investigation of legalization of the funds and property derived from the criminal activity[71]. One of its units, namely Money Laundering Prevention Division of the Analysis and Prevention Board is responsible for prevention and analysis of money laundering and terrorist financing and also serves as Lithuanian FIU[72]. In AML area important rules and provisions are set in orders of the director

70 https://www.infolex.lt/ta/60123?ref=5#Xf11d06c3729d41a6b441ebe842204d13.
71 https://www.fntt.lt/en/money-laundering-prevention/activities/226.
72 *Ibid*.

of Financial Crime Investigation Service[73], guidelines to address issues emphasized in Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing[74], etc. This institution also applies impact measures (fines or warnings) for non-compliance with AML/CFT requirements[75], while its decision may be appealed to national court in administrative case. Another important unit in AML area is the Bank of Lithuania (Central bank) whose function is to carry out the supervision of financial market participants in the area of AML/CFT[76], in year 2021 has supervised 320 units of financial market and imposed over 1,04mil euro of fines for obliged subjects non-compliant with requirements, as well as revoked 2 licenses. Also, a notable unit launched recently in May 2021 is the Center of Excellence in Anti-Money Laundering. This center is a first public-private sector partnership in Europe, operating as separate institution aimed to make in input into a safer financial system in Lithuania by pooling the experience, knowledge and competencies of law enforcement, supervisory and other public authorities and private sector representatives[77].

Supranational bodies, networks and initiatives. With boosting amounts of illicit funds in turnover and intensive attention to ML prevention, emergence of various networks, cooperation and supervision bodies was inevitable.

Supposedly first international formation was established in year 1989 during a G-7 summit in Paris, France as Financial Action Task Force (FATF). The core task of this global inter-governmental body is to set international standards to prevent anti-money laundering on the global level, fueled by unified and coordinated efforts of all countries. FATF shapes policies of AML/CFT, performs monitoring on countries to ensure due implementation of standards and policies in the field, reviews, assesses and in case of need adjusts techniques applied for AML purposes, etc.[78]. As this is a huge worldwide territory, it has nine FATF-style regional bodies (FSRBs) to cover certain regions: APG for Asia/Pacific group, GAFILAT for Latin America, GIABA for West Africa, etc.[79]. FSRBs set up systems and evaluate measures implemented for combatting ML and TF, also proliferation. Whereas the most known work if FATF to date are recommendations – a complete set of counter measures against ML. 40 recommendations on AML

---

73 I. e., Order No 52-V of 24 February 2014 on Supervision of proper implementation of the international sanctions within the limits of competence of the Financial Crime Investigation Service under the Ministry of the Interior, https://www.fntt.lt/en/money-laundering-prevention/legal-acts/legal-acts-of-the-republic-of-lithuania/347.

74 I.e., Guidelines on identifying signs of fictitious entities (in LT language only), https://www.fntt.lt/lt/pinigu-plovimo-prevencija/fiktyviu-imoniu-veiklos-pozymiu-nustatymo-gaires/4112.

75 https://www.fntt.lt/en/money-laundering-prevention/applied-measures-for-breaches-of-the-aml-cft-law/4169.

76 https://www.lb.lt/en/prevention-of-money-laundering-and-terrorist-financing.

77 https://amlcenter.lt/en/.

78 https://www.fatf-gafi.org/about/.

79 https://eurasiangroup.org/en/fatf-style-regional-bodies#:~:text=Eight%20FATF%2Dstyle%20regional%20bodies,FATF%20Recommendations)%20throughout%20the%20world.

were introduced in year 1990, 9 special recommendations on CTF were issued in year 2001 and they all are updated regularly further on. Though recommendations are formally non-binding, countries are expected to comply and closely monitored. FATF monitors jurisdictions on implementation and the ones with weak measures to combat ML and TF are greylisted or even blacklisted as 'jurisdictions with call for action' or 'jurisdictions under increased monitoring'. The ones with call for action are in blacklist and face significant strategic deficiencies in their regimes to counter AML and CFT. On basis of data published on 21 October 2022[80], these include Democratic People's Republic of Korea and Iran, both blacklisted since 2020, also Republic of the Union of Myanmar. Jurisdictions under increased monitoring (the so-called 'grey list') are with the same AML framework problems but cooperating with FATF and committed to resolve their deficiencies in agreed timeframes, thus monitored more closely and regularly. Currently[81] there are 23 countries in a grey list, including so called 'tax heavens' Cayman Islands and Panama, also United Arab Emirates, Albania, Turkey, etc.

MONEYVAL is a FATF-style regional body for European region, independent from FATF but in close cooperation therewith. This is permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism, making recommendations to national authorities in respect of necessary improvements to their systems[82]. Moneyval is composed of 32 jurisdictions, where 32 are evaluated by Moneyval experts, 1 (Israel) by joint group of Moneyval and FATF experts and remaining 2 are delegated to participate by FATF. Moreover, experts of Moneyval supervise and evaluate those countries, who are in the respective region but not members of FATF – currently 28 countries, also 2 non-member states (Holy See and Israel) and additional territories where UK is responsible for international relations (the Isle of Man and Jersey, Gibraltar, etc.)[83]. Lithuania, to note, is not a FATF member, but Moneyval member.

The latest assessment of Lithuania for compliance with FATF recommendations and guidelines as performed in year 2018 during on-site visit by MONEYVAL Mutual evaluation report, later updated in years 2020 and 2021 by 1st and 2nd Follow-up reports. Overall Lithuania has none 'non-compliant' ratings, is fully compliant with 14 FATF recommendations, largely compliant with 21 of them and partially compliant with 5 recommendations[84]. The lowest

---

80 https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2022.html.

81 https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2022.html.

82 https://www.coe.int/en/web/moneyval.

83 https://www.coe.int/en/web/moneyval/jurisdictions.

84 https://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-lithuania-2021.html.

compliance level (still, partly compliant) of October 2021 is shown[85] in respective of Recommendations No. 6 (targeted financial sanctions related to terrorism and terrorism financing), No. 7 (targeted financial sanctions related to proliferation), No. 15 (new technologies), No. 24 (transparency and beneficial ownership of legal arrangements), No. 28 (regulation and supervisions of DNFBPs) and No. 32 (cash couriers)[86]. As a result, Lithuania remained in enhanced follow-up with further duty of reporting back within one year.

One of newest AML policies formators on the EU level is Anti-Money Laundering Authority of the European Union (AMLA EU)[87], created on 20 July 2021 by a comprehensive package of proposals in order to strengthen AML/CFT rules. Rather than monitoring and tackling money laundering activities, AMLA EU will ensure efficient and adequate supervision of obliged entities with high ML/TF risk, strengthen common supervisory approaches for non-selected entities and facilitate joint analyses. The need of formation of this body arose from identified weaknesses of AML/CFT network in the European Union, shown by money laundering schemes and criminals.

On the worldwide scale, the Global Programme against Money Laundering, Proceeds of Crime and the financing of Terrorism (GPML) under the United Nations Office of Drugs and Crime[88] is a global program providing in-depth assistance to countries to build and strengthen their anti-money laundering and countering financing of terrorism (AML/CFT) capacity. Through this tool, the United Nations Office of Drugs and Crime encourages countries to develop policies to counter ML and TF and acts as a coordinator of initiatives carried out jointly by the United Nations and other international organizations. The United Nations Office of Drugs and Crime also holds various knowledge sharing initiatives:

- a knowledge management portal for 'Sharing Electronic Resources and Laws On Crime' (SHERLOC)[89] is the initiative to disseminate the vital information and wide range of professional content relevant to AML/CFT;

- International Money Laundering Information Network (IMOLIN)[90] is Internet-based network assisting governments, organizations and individuals in the fight against ML, financing of terrorism and money laundering. Being developed with the input of international organizations in AML field, the network hosts a database on AML legislation and regulations throughout the world, a library, events calendar and case law database.

---

85 2nd enhanced Follow-up report & Technical compliance re-rating on Anti-Money laundering and Counter terrorist financing measures (Lithuania) November 2021, https://www.fatf-gafi.org/media/fatf/documents/reports/fur/MONEYVAL-FUR-Lithuania-Nov-2021.pdf.

86 https://www.cfatf-gafic.org/documents/fatf-40r.

87 https://www.idnow.io/glossary/amla-eu/.

88 https://www.unodc.org/unodc/en/money-laundering/global-programme-against-money-laundering/.html.

89 https://sherloc.unodc.org/cld/en/st/home.html.

90 https://www.imolin.org/.

Though not exhaustive, the list of cooperation networks will not be complete without EGMONT Group, bringing significance to investigation of AML/CFT offences and inter-agency information exchanges. Egmont group joins FIUs of different countries and provides a safe platform for them to promptly share their expertise and financial experience in cooperated combat of ML, TF and associated predicate offences[91]. Being used for intelligence purposes only, the information travels fast and safely encrypted. This working mechanism is distinct from other means of global information exchange (i.e., diplomatic, international law based, etc.) as prompt and reliable exchange of information is often crucial in investigating offences and chasing laundered funds by instant payments through various jurisdictions and financial institutions.

Due to composure of the thesis, non-governmental institutions, private initiatives and semi-automated/automated tools for conducting AML obligations fall out of scope of the analysis.

Unlike other rapid and exposed crimes, i.e., theft or burglary, money laundering is a long-term multilayered process by which a single individual is rarely directly harmed. An individual or groups of individuals are usually victimized in predicate offences, while cleaning of illicit funds obtained from that predicate offence brings more complex damages to a country or society in general.

[91] https://egmontgroup.org/.

3. JUNCTION OF PRIVACY AND AML

Fundamentally, anti-money laundering and data privacy are wildly divergent. The former depends on the sharing and analysis of data, while the latter calls for minimizing the collection and processing of data. Nonetheless, circumstances when AML and privacy collide and to what extent shall be identified in first subchapter, to be able to proceed further with their legal assessment.

3.1 Privacy related AML measures in business-to-client relationship

As analysis has shown in previous chapters, legal framework is filled with rules and routines to achieve anti-money laundering purposes and guarantee crimeless society or at least closest possible outcome to it. This thesis is aimed to be conducted in a financial sector scope mainly, therefore further investigation will continue on where a perspective or actual client (natural person) may experience a slight touch or a serious interference into his/her privacy when dealing with vendors of financial services. For purposes of analysis a spot of attention will be set on national legislation of a particular selected Member state and further investigation of AML related activities where privacy right of a person is involved will be conducted on basis of Lithuanian AML law and EU regulation, where applicable.

Under Art. 8 of 4AMLD and its subsequent renewals and amendments, entitled subjects are subject to risk-based approach, by which they should identify, assess and understand ML risks to which certain entitled subject is exposed and based on these identified risks and take appropriate AML measures for efficient the risk mitigation. This targeted approach allows entitled subjects to focus on the higher risks and implement basic precautionary procedures on moderate risk cases, avoid replacing unnecessary costs on clients, proactively monitor tendencies in ML schemes and adjust own risk management and mitigation policies thereto, etc.

Furthermore, the above cited article of the directive requests entitled subjects to not only apply AML measures and perform risk assessments, but also have them documented and prepared to be made available to the relevant competent authorities and self-regulatory bodies in the field (Art 8 part 2 of 4AMLD). Therefore, entitled subjects must apply two steps of risk-based approach practice: take appropriate steps of identifying and understanding the ML risks they face in their business activity and also have documented policies, controls and procedures to be able to effectively manage, monitor and mitigate those risks, while the minimum set of the items needed is given in the directive. Risk assessments should be performed not only on the entitled subject as the entity or other type of formation but in respect to every client of that entitled subject or project

implemented, or business activity/new project launched, etc. In addition, risk assessments should be regularly reviewed and updated to adjust policies and procedures to changes of any defining factor.

On relationship with client level, risk assessment is being conducted from starting point at a client reception stage (identification, verification, assessment of ultimate beneficial owner (UBO), gathering of information on nature of business and turnovers, etc.), identifying presence of any red flags[92] and evaluating risk level of the perspective client. To note, UBO identification is obligatory when dealing with legal person (throughout all chain of ownership until all natural persons are recognized at the end of the chain), the scenario with adopting a client-natural person must also coincide UBO with nominal account holder. Deviations include, i.e., money mule cases when accounts are opened with the sole purpose to allow third persons to use accounts for some travels of funds in exchange for payment. Also, if the decision to proceed with long-term financial relationship is adopted, continuous monitoring of client activity related to or performed via the entitled subject for signs of ML is made, especially if the client is of higher risk profile (resident or having business with increased risk territories[93], a politically exposed person (PEP) or his close family members, business activity based on cash payments, etc.).

Customer due diligence (CDD). Article 11 of the directive requests the entitled subject to apply mandatory CDD measures on every client when both establishing a business (with the element of duration[94]) relationship or performing an occasional transaction of types set in the directive.

As a part of risk assessment and an implementation of CDD principle, every client of an entitled subject (i.e., financial institution) must be identified, verified and monitored multiple times during his/her journey with the selected vendor:

- *first*, Know Your Client (KYC) phase of AML programs requires identification and verification or a person on reception procedures while 'onboarding' the client to the institution for continuous financial relationship (i.e., opening of the current or savings account or granting a credit) but also in case of one-time assignment of some financial services to a client. Then, procedure to identify the client is repeated every time the client contacts his/her financial institution and wants to receive some oral or written information on his account payables, balance of account or to initiate payments, etc. It must be stressed, that identification and verification procedures are distinct: identification is receival of information on identity of the client and

92 Various circumstances which should put an entitled entity on alert.

93 As provided in Art. 18a of 4 AMLD and listed in Annex I of 4 AMLD, with subsequent amendments and additions.

94 Business relationship – a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration (Article 3 part 13 of 4AMLD).

verification is further check of the information received, performed on a basis of written proof (documents), official registries, etc. Identity is proven by presenting valid personal identity document (passport, personal identity card, driving license (though in some Member states this type of document is not admissible in certain financial institutions for identity purposes), allowance for permanent residence, etc.) – as long as the document is official (government' issued) and contains necessary information. In addition, a KYC questionnaire is required to fill when the client starts relationship with financial institution and later on regular basis, with frequency dependent on risk level of the particular client. In all these actions a client – natural person is required to give the vendor personal data for further processing: name, surname, personal code, residence address and other contact details, followed by some personal financial information (source of income, expected turnover amounts through the account, destinations where to and where from funds will be transferred, purpose and intended nature of the business relationship, etc.). To note, some requests for information may be qualified as short in precision, for example, what is your planned/expected income amount in next year period, as the client may expect anything he/she pleases to and generally bears no responsibility for derogation from reality. Despite destinated to red flag deviations and abnormal operations in the client account, this question would technically produce red flag almost every time when yearly income accumulative will deviate from planned amount in as little as 1 euro amount. Therefore, it can be assumed, that questions of this type put in KYC questionnaires are inappropriate for AML monitoring purposes in absence of human participation;

- *second,* in case of a continuous relationship, entitled subject of a financial sector has to periodically re-check if the KYC information about the client is up-to-date (by refreshing KYC questionnaires and personal identification data and documents in case of changes), perform sanctions scans and monitor operations or absence of them to evaluate, whether it is typical conduct for the client, are operations compliant with general AML requirements, request additional information and written proof in need of additional verification of financial activity, etc.;
- *finally*, CDD measures are applied each and every time the client performs or asks his financial vendor to perform the transaction (as a part of transactions monitoring activities), in order to understand the reasoning behind the instructions the client gives. In addition to verification of identity of a person, the entitled subject shall check whether UBO of the transaction is known and what is the purpose and intended nature of this transaction. Generally, circumstances with obligatory CDD procedures for the occasional transaction are listed in article 11 of 4AMLD (threshold of 15thou euro or more for a transaction in single operation or multiple linked operations, threshold of 2thou euro and more for a collection of winnings or/and wagering the stake transactions for providers of gambling services, etc.).

As a general rule, CDD must be performed before the business relationship with the client or an occasional transaction is started, although Member states may allow simultaneous verification procedures of the client and UBO along with business activity, if necessary. It should, however, be evaluated, that in case of discrepancies of verification procedures, parallel business activity will already be partially performed and formally non-compliant with AML purposes.

Whereas AML activities are risk based, depending on the level of risk there are two levels of CDD available: simplified due diligence (SDD) for low risk profile clients and enhanced due diligence (EDD):

- in case of low probability of money laundering or terrorist financing in business relationship or occasional transaction with the client, the identification and basic amount of information is needed: name, address, phone number, employment background, place and date of birth, personal code, residential address, marital status, names and other identification data of close family members, past criminal record (if any), etc. Annex II of 4AMLD provides a list of circumstances of three types (customer type, transaction type and geography), when potentially lower risk can be decided and can lead to SDD. For example, in low-risk geography factors are present registration, establishment and residence cases in Member states, third countries having effective AML/CFT systems, third countries identified by credible sources as having a low level of corruption or other criminal activity and third countries having requirements to combat ML and TF consistent with FATF recommendations and effectively implementing those requirements (Annex II part (3) of 4AMLD). Once the relationship is established and periodical KYC checks are performed, some trigger events may arise resulting in changed risk level and need for additional due diligence procedures, therefore changed type of CDD;
- when risks are higher than in SDD cases, especially the ones set in article 18 of 4AMLD are obviously present, EDD must be conducted. It usually happens with transactions that are complex, unusually large in amounts, conducted in unusual pattern (i.e., split to amounts approaching but not exceeding amount threshold for reporting to authorities or transit payments[95]), without apparent economic or lawful purpose or are otherwise primarily suspicious. Again, a non-exhaustive list of factors that indicate a potentially higher risk and need for enhanced due diligence procedures is presented in Annex III of 4AMLD. Factors are divided into three categories – customer type, transaction type and geography, for example, geography section encompasses countries identified by credible sources as not having effective AML/CFT systems, having significant levels of corruption or other criminal activity, being subject to sanctions, embargos or

[95] Transit payments – situations when funds enter the bank account and are transferrred to different account in a short period of time. If no other transactions are performed in that bank account and transit payments prevail, this constitutes the criteria for suspicion.

similar measures issued by international authorities and the ones who provide funding or support for terrorist activities or have designated terrorist organizations operating within their territory (Annex III part (3) of 4AMLD). Actually, all PEPs in the role of clients or UBOs of the clients, sanctioned clients, cash intensive businesses, companies with complex ownership structures or nominee shareholders, residents of geographical areas of higher risk fall into EDD scope. In addition to the amount information gathered as in SDD case, EDD requires more, in example, more than one valid external document for identity verification to verify not only the client, but also UBO if they do not coincide. Additional due diligence activities, such as exhaustive analysis of wealth sources of the perspective client including accounting results, adverse media checks, potential on-site visits in case of business entrepreneurs are implemented.

Obviously, most of the above listed information in scope of natural persons being clients themselves or representatives, shareholders or UBOs of corporate clients, is personal data protectable under GDPR. Therefore, obliged subjects are in full responsibility for due processing of personal data. To note, article 25 of 4AMLD allows obliged subjects to rely on reliable and controlled by directive third parties to meet CDD requirements but plants the ultimate responsibility for meeting CDD requirements on the obliged entity which relies on third party. Simultaneously, the sole responsibility for data processing of clients'/their family members' personal data in compliance with GDPR remains with obliged entity.

Record keeping. Along with activities aimed at verification of the identity of the client and ensuring his/her transactions are compliant with AML requirements, AML directives impose a duty on obliged subjects to keep records for 5 years after the end of a business relationship with the client or after the date of the occasional transaction (Art. 40 of 4AMLD). The 5 years term is a minimum period covered by AML directive; therefore Member states may extend it in domestic legislation, but in any case should not exceed 10 years period. Records that must be kept include historical proof of CDD activities and identification of transactions. As for CDD part, copies of the documents and information that are (was at the time) necessary for the obliged entity to comply with CDD requirements, in both material (hard copies) and electronic forms must be kept. Regarding the transactions, records include supporting evidence of transactions consisting of the original documents or copies admissible under the applicable national law, necessary to identify performed transactions, generally the ones that would allow to reconstruct the individual transaction. After a record keeping period is over, all data kept must be deleted fully.

3.2. Privacy exposures in external processing of AML-related personal data

In general, entities and governmental organizations bear a great load of responsibility to gather, process and keep personal data in compliance with GDPR. In addition to clear out rules and procedures on selecting data that are essential and justifiable to process, subjects face responsibility to the proper protection of data both on inside level and outside the entity. If any of processed data are shared with third persons, GDPR implies strict rules on legislation or contractual basis on how it must be done. In addition, the effectiveness of AML measures is directly and closely dependent on exchange of information between multiple subjects and beyond national jurisdictions.

The abovementioned explanation on processing personal data for AML purposes exceeding the internal scope of processing activities, allows to identify two main types of external processing: obligatory AML reporting to relevant authorities and voluntary sharing and publishing of personal data necessary for AML purposes.

Reporting obligations. The principal obligation of actions to be taken by the obliged subject, including their directors and employees in particular, if a suspicious transaction is found, comes from article 33 of 4AMLD. In case the subject 'knows, suspects or has reasonable grounds to suspect' that funds under transaction are the proceeds of criminal activity and participate in ML schemes or are related to TF, he needs to promptly inform the domestic Financial intelligence unit (FIU) on the situation by filing a report, also proceed in full cooperation by responding to FIU requests for additional information, providing FIU directly with all necessary information and remain confidential of actions performed in respect of suspected client/transaction initiator (anti-tipping off provision in Art. 39 of 4AMLD) and third persons. All suspicious transactions including their attempts must be reported. In case of filing the report, the obliged subject is required to sustain from carrying out transaction and withhold the suspicious funds until further FIU decision is taken or instructions received. While performing their duty to report suspicious transactions to FIU, obliged subjects and their particular employees fill in the Suspicious transaction report (STR) in standardized form that may vary one Member State to another Member State and is generally of FIU admissible content. Among other data that are needed to fulfill reporting duty and necessary for FIU to take a decision on whether to commence a further investigation, are personal data of a client or transaction initiator that was met by the obliged subject during a reportable activity. In essence, name, surname, contact details, other relevant details as to client business profile or information on reasoning of operation that the client tried to initiate are transferred to FIU.

Data sharing inside and outside the EU. As is set in Art. 4 of GDPR, a 'cross-border processing' is processing of personal data in a way when either data controller or data processor are established in more than one Member country of the EU, or data is processed in one country, but processing substantially affects or might affect one or more data subjects in more than one Member country. In both mentioned situations data does not leave the EU territory. Oddly enough, some Member states have gone beyond the minimum requirements scope but by different methods, in example, the content of STR form may vary in different Member states, etc. Also, specific challenges as to assigning third parties for CDD purposes, foreign language of the documents containing personal data and their literate translation issues, etc.

Nevertheless, for data travels *outside* the EU territory GDPR has its own provisions. Art. 44 of GDPR clearly states that any transfer of personal data for current of upcoming processing in third country or international organization may be performed only if provisions laid down in Chapter V of GDPR are complied with, but also in a manner compatible with main GDPR principles of data processing (fairness, lawfulness, data minimization etc.). The abovementioned chapter, inter alia, provides three bases to transfer personal data: an adequacy decision (Art. 45 of GDPR), appropriate safeguards (Art. 46 of GDPR) and derogations for specific situations (Art. 49 of GDPR). One of core principles when transferring personal data to third countries is also request to ensure continuity of personal data protection, irrespective of the fact that receiver (country of residence of the receiver) is outside the EU and subsequently outside the regulative scope of GDPR. It is notable, that allowing access to processed personal data to third parties always constitutes an interference to human right enshrined in article 7 of the European Charter on Human Rights, as it was found multiple times by CJEU (the communication of data to public authority – PNR case[96], etc.). For interference to be permissible, certain conditions must be met and further analysis of this is given in chapter 4 of this thesis.

Notwithstanding the above said and concluded, there is still a certain discrepancy in legislation regarding personal data sharing. As presented above, 4AMLD requires obliged subjects to share customer data with foreign regulatory bodies, but GDPR generally bans personal data-sharing with third countries. Notably, GDPR provides possibility of data transfers for important reasons of public interest, but this criteria is rather broad and not clearly defined. Possibly, the biggest challenges are faced in jurisdictions where processing of customer data outside the country is restricted or even forbidden[97]. It was already mentioned multiple times during this research that effective AML framework needs support of cooperative government, supervision bodies,

96 CJEU, PNR Opinion 1/15, ECLI:EU:C:2017:592, Judgement of 26 July 2017.

97 Nick Parfitt. AML Compliance – Data Privacy challenges. *Risk & Compliance*, July 2019: 4, https://www.acurisriskintelligence.com/assets/RC_JUL19%20REPRINT_ACURIS_AML.PDF.

authorities (FIUs) and obliged subject to timely share information on updated ML typologies, vital data on movements of suspicious funds etc. Restrictions or even unavailability or extraterritorial movement of personal data would severely reduce success of combatting ML.

Sanctions lists. Governments and international organizations publish lists of subjects (people, groups, entities) who are engaged in criminal activities, including ML and TF. Subjects in these lists are imposed various sanctions – restrictions and negative consequences as to their business activity, freedom of travels, ownership etc., therefore lists are commonly named 'sanctions lists'. Obliged entities must include sanction lists scanning in their CDD procedures to avoid onboarding a sanctioned subject for a permanent relationship or accidental transaction, also to monitor whether an onboarded client was not sanctioned during the period of relationship with obliged subject. Generally, blocked persons are forbidden to make any transactions and sanctions scanning is a vital routine in a financial sector entities.

Overall, there are many different sanctions lists and in particular the ones with individuals included, for example[98], consolidated sanctions lists of particular countries (UK sanctions list, Canadian autonomous sanctions list, US sanctions list etc.), international organizations (United Nations Sanctions[99], OFAC – Specially designated persons' list, Interpol Wanted, etc.) or territorial-political organizations (EU financial sanctions[100]), also lists where entries are gathered and sorted by type of sanctioned individuals (Every politician PEP list, World presidents PEP list, etc.). In respect of individuals, participation in any of these lists means disclosure of personal information in the scope allowing to identify the person and impose certain measures on him/her. In other words, publishing of AML related and necessary data to achieve general purposes of combatting ML is processing personal data of list entries (individuals) by publishing them in free access to a society.

Whistleblowers. Article 61 of 4AMLD requires presence of safe, prompt and effective channel to report potential or actual breaches of national laws where AMLDs are transposed for employees or persons in a comparable position of obliged subjects to report breaches internally. Although whistleblowing still is reporting activity, personal data in this type of reporting does not cross the borders of the obliged subject. Probably compliance with data minimization principle and adequacy of access rights to these data could be investigated.

Audits, legal advisory, etc. While providing auditing, legal and other consultancy services, third parties may be exposed to AML related data, including personal data. Though this is also data sharing cases, the mentioned third parties should be treated as data processors (or data

98 https://sanctionscanner.com/blog/what-is-a-sanction-list-8.
99 https://scsanctions.un.org/9v1k8-en-dprk.html#alqaedaind.
100 https://www.sanctionsmap.eu/#/main.

controllers in exclusive cases) and fall out of scope of the research on personal data publishing/sharing purely in AML framework.

As expressed above, personal data of a prospective abuser of AML rules may be processed equally in internal and external areas. In significant part of those cases the data subject is not the source of his data, did not presented consent for gathering, use and sharing of his/her data and even lacks awareness of any actions towards his/her data at all. To say more, data subject has no influence as to for how long, how exhaustive and how safe personal data are processed, although even in case a privacy right is interfered with authorization of law, data subject retains a right to suffer restrictions in a scope not exceeding and deviating the limits prescribed. This rivalry of interests – personal and public ones – requires clarity and balance between legal provisions of privacy and AML to execute provisions in equally respectful manner for both virtues.

4. PROPER IMPLEMENTATION OF PRIVACY RESTRICTIONS IN AML

The existence of two or more contradictory interests leads to legal tension, risks of deviant court decisions in similar disputes and finally, inefficiency of legal provisions. According to Keil and Poscher[101], one form of indeterminacy called 'vagueness' may be caused from the use of value predicates like 'reasonable' and 'excessive'. Disbalance in ratio of these value predicates leads imminently to disbalance in protected interests. In scope of this research, analysis will be continued as to when and why interference into or restrictions of privacy right for AML purposes is reasonable, thus permissible and when it becomes excessive.

It must be noted that legal provisions were developed towards defining on how data should be processed (authorized processing) and under what conditions deviations from authorized processing are permissible (restrictions or interference into privacy).

The Charter of Fundamental Rights of the European Union (2000) clearly states in article 8 (2) that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on other legitimate basis laid down by law. CJEU has explained, that if personal data are processed in compliance with the abovesaid article, there is no interference into *right for data protection*, but private life may be still interfered by collection, storage or disclosure of such data, therefore justification is needed[102]. Whereas general limitations to human rights, a right to privacy included, can be found in article 52(1) of this document where it is said: **limitations must be provided for by law, respect the essence of the affected right and by the principle of proportionality, must be necessary and genuinely meet the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others**. It can be assumed that existence of one of listed circumstances to apply limitations justify the interference into private life. To note, the right of a person to be aware who processes his personal data, what data and for what reason, as set in last sentence of article 8 (2) of this Charter and transferred to respective article of GDPR (see below) falls into scope of human rights under applicability of general limitations rule. In other words, the Charter has set grounds for tipping-off rule that will be directly legislated some fifteen years later.

GDPR as the piece of legislation is devoted for the protection of personal data and privacy rights. Nevertheless, it also allows Member states to create legal provisions for restrictions, 'when such a restriction constitutes **a necessary and proportionate measure** in a democratic society to

---

101 Geert Keil (ed.), Ralf Poscher (ed.), *Vagueness and Law: Philosophical and Legal Perspectives*. Oxford University Press, 2016: 49.

102 CJEU, joined cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert, ECR I-11063; European Court of Human Rights case Amann v. Switzerland, App No. 27798/95, ECHR 2000-II; European Court of Human Rights case Amann v. Switzerland, App No. 28341/95, ECHR 2000-V.

safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories' (part (19) of Preamble of GDPR).

Corresponding criteria are observed in domestic law that had to implement EU principles by manner of transposition or relevant adjustments. For example, according to Art. 22 part 3 of the Constitution of the Republic of Lithuania, any information on private life of the individual can be gathered (that is, intervened) only on the basis of the reasoned court decision and compliant with legal provisions. Generally, three criteria should be met to interfere: i) state support, and ii) lawfulness, and iii) justification.

AML directives also enclose provisions on data protection. Namely, article 41 of 4AMLD obliges to process personal data only for purposes of the prevention of ML and TF, also forbids further processing in a way that is incompatible with those purposes, clearly prohibiting obliged subjects to perform data processing for any other purposes, *inter alia*, commercial needs, marketing or profit. Moreover, under provisions of 4AMLD, new clients shall be provided necessary information under GDPR (including notice on obligation of obliged subject to process personal data for AML purposes) prior to establishing the business relationship or conducting the occasional transaction. This gives reason for conclusion that legal basis of obliged subject to process personal data of the client is not a client' consent. Irrespective of the consent is or is not obtained, the legal basis should be identified from Art. 6 of GDPR where all lawful bases are listed. It may be concluded that two bases may be applied to data processing when it is done by obliged subject for AML purposes:

- processing is necessary for compliance with a legal obligation to which the controller is subject ((Part (c) Art. 6 of GDPR), and
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ((Part (e) Art. 6 of GDPR).

The first legal base derives from Art. 40 of 4AMLD where the *obligation*, *duty* of the obliged subject to process certain personal data for AML purposes is provided. Second legal base fits the article 43 of 4AMLD that equates data processing for AML purposes under 4AMLD to the matter of public interest under GDPR.

In addition, the anti-tipping-off duty as said above is a clear exception of general right to be informed about one's personal data processing. While article 13 of GDPR holds excessive explanations as to how, when and by what information data subject must be kept aware of his/her data processing activities, none of them is applicable in case the obliged suspect lodges an STR to

FIU on suspicious transaction initiated by or with participation of that data subject. To say more, this exception is so significant for AML as matter of public interest, that it was readily inserted into GDPR under article 23 where restriction to the right of access to data is directed into framework of AML - the restriction should be a necessary and proportionate measure to safeguard national security, public security, defense, prevention, investigation, detection or prosecution of criminal offences, etc.

Based on the above listed exceptions to comprehensive protection of a privacy right by legislation, interference to privacy right (or limitations of privacy right) is permitted only if both conditions are met: 1) lawfulness, and 2) justification.

Lawfulness or legal basis**.** A limitation of a right to privacy must be based on valid reasoned court decision or legislative piece, where certain limitation is grounded (i.e., article 23 of GDPR). A restriction is never applied if not backed up by legislation, otherwise the scope and severity of limitations based on common sense, good intentions or other grounds would probably exceed any limits. Moreover, a limitation may derive only from valid law, directly applicable to the data subject, if all conditions listed in legislative piece are met.

Justification. A general reference to public interest is not sufficient to justify restrictions on privacy right. According to legislation, following cumulative components of justification can be distinguished:

- *proportionality*. The intended benefit of combating money laundering has to be weighed against citizens' freedom and data protection and stay balanced. The proportionality principle itself derives from article 5 of the Treaty on EU[103] and means that the action of the EU must be limited to what is necessary to achieve the objectives of the Treaty. Though by the Protocol No. 2 of the Treaty the proportionality principle was expanded to Member States and EU level legislation scope, the soul of the principle may be explicitly comprehended. Proportionality principle is widely acknowledged in AML framework, for instance, the European Data Protection Supervisor (EDPS) in its Opinion of 2 February 2017 on a Commission proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC[104] has expressed its concern to the European Commission that FIUs should open investigations not on sole basis of received STRs, but based on results of their own intelligence and analysis, also that legislative provisions on significantly broad access to beneficial ownership information by both competent authorities and general public is disproportionate for the alleged aim of optimizing enforcement of tax obligations. By this and other notes the institution pointed out possible deviations from proportionality principle in AML

[103] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E/PRO/02&from=EN.

[104] EDPS Opinion of 2 February 2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC, Access to beneficial ownership information and data protection implications / https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf.

area. According to EDPS, processing personal data for purpose A that were indeed collected for purpose B, completely unrelated purpose infringes the data protection principle of purpose limitation and threatens the implementation of the principle of proportionality. As to justification of interference of privacy right, no doubts exist that level and scope of restriction must be directly dependent on achievable purpose, therefore proportionate in categories of 'sacrifices and gains'. The explanation on how proportionality principle shall be achieved is also presented by CJEU: *'the protection of the fundamental right to respect for private life on EU level requires [...] that derogations from and limitations on the protection of personal data should apply in so far as is strictly necessary. [...] The legislation must lay down clear and precise rules governing the scope and application of the measure [...] and imposing minimum safeguards so that a persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against a risk of abuse'*[105];

- *necessity.* Definition of necessity is not separately set in legislation and usually is presented through and used in accordance with the request of proportionality. While checking the necessity of AML measures, the assessment created by CJEU[106] should be repeated, namely checking if limitations on privacy right are strictly necessary and whether the provisions enshrining the limitation provide clear and precise rules on scope and application of the measure, as well as safeguards on proper execution of the limitation;

- *clarity in definition.* Any limitation of the fundamental right can be justified only if its definition is clear, concise and cannot be interpreted in broadest sense. The clarity of legal norms necessarily calibrates conflicting values, keeps legislative expectations close to the direction of actions and contributes to reign of right decisions over mistaken ones. Inconsistent, misleading AML terminology and in particular definition and scope of limitation of a fundamental human right would lead to discrepancies in procedures and excessively negative consequences both to data subject and data processor. As CJEU explained in Schrems case, the legislation must lay down *clear and precise* rules governing the scope and application of measure that constitutes the interference into privacy right.

Nevertheless, key principles of personal data processing should also be retained to ensure proper data processing when privacy right was interfered by gathering, use, sharing and other processing activities of personal data:

- *lawfulness, fairness and transparency*. Lawfulness of data processing is set in article 6 of GDPR and mainly determines whether there is a legit ground for data processing. A more extensive research as to what grounds are used for data processing for AML purposes has been

105 CJEU, PNR Opinion 1/15, ECLI:EU:C:2017:592, Judgement of 26 July 2017.
106 *Ibid.*, and others.

done above. Fairness is unfortunately not defined in GDPR and should be understood by general sense as the way of treating equally or in a way that is reasonable[107]. Whereas transparent data processing is the one where data subject is informed about his data processed in a form that is easily accessible and easy to understand (part (39) of Preamble of GDPR). It was already explained that AML area hosts a specific limitation to this principle, the tipping-of prohibition;

- *purpose limitation.* Data should be used for explicit, legit and specified purposes only and it derives from part (33) of Preamble of GDPR. In AML area personal data are meant to be processed for ML prevention, combatting and investigation purposes only, avoiding fellow purposes like marketing, automated scoring, etc.;

- *data minimization*. Obviously the principle 'the more we know, the safer we feel' can not be applied in scope of GDPR regulation. Data processed should be limited to the extent that is necessary for purposes of data processing, namely, AML measures.

- *accuracy.* Personal data must be accurate and updated if possible. In AML area inaccurate, fragmental or outdated information about an individual could lead to negative direct consequences suffered by data subject, i.e., withhold of funds of transaction, inclusion of an individual into sanctions list, etc.;

- *storage limitation.* This principle requires storage of personal data without excessive periods after purposes of data processing were reached. AML sector participants have legitimate expectations for their personal data be kept archive for no longer than is necessary for AML purposes;

- *integrity and confidentiality.* A processor must ensure the appropriate security level of personal data processed, protection from unauthorized use, accidental loss or damage. Exceptions of confidentiality principle for data processors in AML area were elaborated on above in AML data sharing and publishing section of the thesis;

- *accountability*. Article 5(2) of GDPR insists that a processor shall not only stay compliant with GDPR requirements but also be able to prove its compliance if needed. In other words, as long as the organization clearly documents the purpose for which the data is being used and adheres to its controls to ensure the appropriate access, there should be no conflict between the data privacy and AML data usage[108].

Perhaps the most illustrative example of judicial evaluation of interference into right to privacy and application of abovementioned criteria and principles is a recent CJEU decision on joint cases of *VM and Sovim SA*[109], rather known as 'UBOs case'. In disputes, CJEU evaluated the

---

107 https://www.oxfordlearnersdictionaries.com/definition/english/fairness.

108 *Supra note* 97: 3.

109 CJEU, Judgement of 22 November 2022, WM and Sovim SA (Joined cases C-37/20 and C-601/20, EU:C:2022:912).

provision of article 30 of AMLDs as to the full access granted to every member of the public to personal data of UBOs in state registries in respect of the right to private and family life and the right to protection of personal data as set respectively in articles 7 and 8 of the Charter of Fundamental Rights of the EU (further referred to as 'fundamental rights'). CJEU found that making personal data accessible to public constitutes interference with the questioned fundamental rights, whatever the subsequent use of information communicated. Then, the court also recognized as interference the circumstance that the possibility is created to use published personal data of UBOs for whatever purposes without control, as data are publicly available. While CJEU acknowledged that condition of lawfulness exists and the essence of the fundamental rights was not undermined, the principle of transparency cannot be considered a general interest and justify the interference into fundamental rights. Furthermore, the court found the disputed provision of AMLDs as not limited to what is strictly necessary. By CJEU opinion, even the exemptions from the provision allowing registered entities on the basis of duly motivated 'exceptional circumstances' to demand the manager of the beneficial ownership register to limit the access of UBOs information only to certain persons, such as national authorities and credit/financial institutions, are inefficient to demonstrate a proper balance between suppressed fundamental rights and the objective of general interest pursued. Based on these findings, CJEU recalled a relevant part of the article of AMLDs that was disputed.

Besides the above listed conditions and principles, it should be considered that certain sensitive data elements construct a special categories data, such as person's sexual orientation or health status. As the European Court on Human Rights has emphasized, *'the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of data'*[110] and, naturally, the bigger responsibility of data processor. Given extra complexity in processing these data introduced by GDPR, appropriateness of using them for AML purposes should be double, if not triple-weighed. Moreover, it should be highlighted that these special categories data are not necessary for the obliged subject to identify or verify the client or for investigation authority to analyze the suspicious transaction. They might, but not must, give extra information on reasons of probable participant or organizer of ML activities, but not constitute essence of the crime itself. For example, a person can be more vulnerable to be included or more open to violate provisions of law if suffers from serious or fatal illness, but these circumstances are rather impactful for criminal investigator or the court to adjust his liability, selecting an appropriate penalty for

[110] European Court of Human Rights case M.M. v. UK, App No. 24029/07 (13 November 2012).

predicate offence separately or ML crime in general, but not for investigation or qualification stages of his unlawful actions in respect of criminal law.

To sum up the analysis performed in this chapter it can be concluded that any collecting, use and sharing of personal data for AML purposes is the interference into a right to privacy and/or right to data protection, constituting a limitation of these rights accordingly. The interference into fundamental right is permissible if does not breach the essence of the right, is lawful, proportionate and necessary for achieving certain purposes, justifying the interference into privacy as a sacrifice. The requirement of appropriate justification may be divided into requests for the interference (restrictive measure in AML sector) to meet principles of necessity, proportionality and clarity in definition. In addition to meeting conditions of permissible interference into privacy rights, the processing of personal data for AML purposes must comply with applicable principles of data processing as set in GDPR.

CONCLUSIONS AND RECOMMENDATIONS

Based on the research conducted, several conclusions can be drawn by summing up the main points made in this thesis:

1. The right to privacy is a fundamental, though not absolute human right. Global legislation on human rights allows the interference into, violation or deprivation of privacy right in cases where certain conditions are met, including basis on reasoned judicial decision or regulation by law.

2. The concept of right to privacy is still evolving in sense of its boundaries, as judicial jurisprudence is constantly shaping them by deciding whether this right was infringed in various disputable situations. Nevertheless, even if found, the infringement is not in itself negatively consequential to the abuser if interference was compatible with conditions of its application set in human rights and AML legislation.

3. Protection of privacy and application of AML mechanisms are directly contradictory, but still compatible under certain criteria. Even though, the full extent of privacy is never reachable when ensuring AML purposes. Governments and the society at large have prioritized a protection of the legal value of higher rank, sacrificing full privacy to effective AML prevention and combat.

4. The EU legislation on human rights allows limitations of fundamental rights, a right to privacy included, when the essence of the right is not breached, the interference is lawful, proportionate and necessary for achieving certain purposes, by this justifying the permissible interference. Legal basis needs to derive from legislative piece or reasoned court decision, while justification is achieved by restrictive AML measures being proportionate, necessary and concise in definition.

5. Data processing activities in AML are not based on consent of the data subject, as the subject may not or must not, in case of tipping-off prohibition, be aware of such data processing. Rather than that, grounds are necessity to comply with legal obligation or/and duty to perform for sake of public interest or executing official authority and they constitute a specific regulation in respect of GDPR. Besides, data must be processed transparently, accurately, with purpose limitation and in compliance with other processing principles set in GDPR.

6. Cumulative principles of lawfulness and justification balance two contradicting virtues and constitute 'a litmus test' to current legislation in AML area. Any legal provision lodging legit interference into privacy but failing to maintain justification leads to declaration void, as happened in CJEU case on public access to personal data of beneficial owners of entities.

Based on results of conducted analysis and own deliberations, the following recommendations may be offered:

1. As recent event of CJEU banning the public disclosure of ultimate beneficial owners' personal data has shown, preventive measures in AML field may fulfill security needs of a society at large but still be found disproportionate to suppression level on the right of individual. Overall, findings of this thesis indicate that a wider and more complex European-level scientific research initiatives are needed to develop and constantly facilitate the awareness of fundamental human rights being in contact with ML and TF prevention initiatives. Full and timely involvement of legal science is crucial help to keep balance between contradicting virtues without temptation to prioritize the one that tackles more pressing problems at that period.

2. In constant evolution of financial wrong-doers and legal frameworks, regulatory and legislative bodies of the AML area are to face even bigger challenges in search for a proper balance between privacy protection and efficient ML prevention. While no significant problems with lawfulness of AML measures are expected, aspect of their justification will play the key role in survival of these measures, increasing weight of proportionality checks and proper recognition of general interest in presence. Thus balance test for weighing the restriction level of privacy right (sacrifice) and objective being pursued by AML measure (gain) must be done very thoroughly, on the basis of concepts and methodologies developed by legal scholars *prior to* introduction of the measure, but not as control mechanism by judicial system in case of subsequent disputes.

REFERENCE LIST

NORMATIVE SOURCES

1. The Universal Declaration of Human Rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights.
2. Consolidated version of the Treaty on European Union, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF.
3. Protocol No. 2 of the Treaty on EU on the application of the principles of subsidiarity and proportionality, https://euro-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E/PRO/02&from=EN.
4. Charter of Fundamental Rights of the European Union, https://euro-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
5. European Convention on Human Rights, https://www.echr.coe.int/documents/convention_eng.pdf.
6. Resolution adopted by the Human Council on 16 July 2012 on the Promotion, protection and enjoyment of human rights on the Internet, https://digitallibrary.un.org/record/731540?ln=en.
7. Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (1AMLD), https://euro-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31991L0308&from=FR.
8. Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (2AMLD), https://euro-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001L0097&from=EN.
9. Directive 2006/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (3AMLD), https://euro-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0060&from=EN.
10. Directive 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 (4AMLD), https://euro-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

11. Directive 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 (5AMLD), https://euro-lex.euroopa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN.
12. Directive of the European Parliament and Council of 20 July 2021 on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849 (6AMLD), https://euro-lex.euroopa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0423&from=EN.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://euro-lex.euroopa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.
14. The Constitution of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=rivwzvpvg&documentId=TAIS.211295&category=TAD.
15. Civil Code of Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495.
16. Law of the Republic of Lithuania on Money laundering and terrorist financing prevention, https://www.infolex.lt/ta/60123?ref=5#Xf11d06c3729d41a6b441ebe842204d13.
17. Law on restrictions of cash payments of the Republic of Lithuania as of 23 June 2022, https://www.infolex.lt/ta/780418.

CASE LAW

1. European Court of Human Rights case M.M. v. UK, App No. 24029/07 (13 November 2012).
2. European Court of Human Rights case Amann v. Switzerland, App No. 27798/95, ECHR 2000-II;
3. European Court of Human Rights case Amann v. Switzerland, App No. 28341/95, ECHR 2000-V.
4. CJEU, joined cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert, ECR I-11063.

5. CJEU, Judgement of 22 November 2022, WM and Sovim SA (Joined cases C-37/20 and C-601/20, EU:C:2022:912).
6. CJEU, Judgement of 13 May 2014, Google Spain and Google (C-131/12, EU:C:2014:317).
7. CJEU, Judgement of 9 November 2010 Volker und Marcus Schecke and Eifert (C-92/09 and C-93/09, EU:C:2010:662).
8. CJEU, Judgement of 17 October 2013, Schwarz (C-291/12, EU:C:2013:670).
9. CJEU, Joined Cases C293/12 & C594/12, Dig. Rts. Ir. v. Minister for Comm., ECLI:EU:C:2014:238, Judgement of 8 Apr. 2014.
10. CJEU, Case C362/14, Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650, Judgement of 6 Oct. 2015.
11. CJEU, Case C-203/15, Tele2 Sverige AB v. Post-och Telestyrelsen, ECLI:EU:C:2016:970, Judgement of 21 Dec. 2016.
12. CJEU, Case C-817/19, Ligue des droits humains v Conseil des ministres, https://curia.euroopa.eu/juris/document/document.jsf?text=&docid=264843&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=8500
13. The European Court of Human Rights, case Samoylova v. Russia, Application No. 49108/11 / *https://hudoc.echr.coe.int/eng?i=001-213868*
14. The European Court of Human Rights, case Solska and Rybicka v. Poland, Application Nos. 30491/17 and 31083/17 / *https://hudoc.echr.coe.int/eng?i=001-186135*
15. The European Court of Human Rights, case Jivan v. Romania, Application No. 62250/19 / https://hudoc.echr.coe.int/eng?i=001-215475
16. EDPS Case Law Digest: transfers of personal data to third countries / https://edps.euroopa.eu/system/files/2021-06/21-06-09_case-law-digest_en.pdf
17. Guide on Article 8 of the European Convention on Human Rights (updated 31 August 2022) / https://www.echr.coe.int/documents/guide_art_8_eng.pdf

SPECIAL LITERATURE

1. Cassella, S. D. 'Reverse money laundering'. *Journal of Money laundering control*. London, Vol. 7 (1), Summer 2003. / https://www.proquest.com/docview/235831715.
2. Ciesiolka M. *Protecting the Right to Privacy while combating Terrorist Finance*. August 5, 2019. https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/Sub-missions/Mirja_Ciesiolka_GA74CT.pdf
3. Ciriani V. *et. al*. *Theory of privacy and anonymity*. University of Milan, 2013. https://www.researchgate.net/profile/Valentina-Ciriani-

2/publication/228707386_Theory_of_privacy_and_anonymity/links/545949dd0cf2bccc4912ba17/Theory-of-privacy-and-anonymity.pdf

4. Keil G. (ed.), Poscher R. (ed.). *Vagueness and Law: Philosophical and Legal Perspectives*. Oxford University Press, 2016.
5. Khartit K. *How do prepaid cards work?* April 30, 2021 / https://www.investopedia.com/ask/answers/042315/how-do-prepaid-debit-cards-work.asp
6. Kokott J., Sobotta C. 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR'. *International Data Privacy Law*, 2013, Vol. 3, No. 4. P. 222-228.
7. Laurinaitis M. *Elektroninių pinigų teisinis reguliavimas* (doctoral thesis, 2015) / https://repository.mruni.eu/handle/007/14384.
8. Lytvinenko A. 'The legal approaches of defining the equipoise between privacy and public interest'. *Teisė*, 2017 / https://www.zurnalai.vu.lt/teise/article/view/10525/8881.
9. Humpfrey D., Khiaonarong T. *Cash use across countries and the demand for Central Bank Digital Currency*. IMF Working paper WP/19/46, 2019. https://www.imf.org › Files › WPIEA2019046.
10. Maxwell G. *The first successful Zero-Knowledge Contingent Payment.* https://bitcoincore.org/en/2016/02/26/zero-knowledge-contingent-payments-announcement/
11. Maxwell G. Coinjoin. 'Bitcoin privacy for the real world'. August 2013. *Bitcoin Forum*. https://bitcointalk.org/index.php?topic= 279249.0, 2013.
12. Meškauskaitė L. 'Asmens teisių apsauga ordinarinėje teisėje: teorija ir neišnaudotos galimybės (The protection of individual rights in ordinary law: theory and missed opportunities) '. *Asmens teisių gynimas: problemos ir sprendimai (mokslo studija) (The protection of individual rights: problems and solutions (scientific study)*). Vilnius: Mykolas Romeris University, 2014. ISBN 978-9955-19-694-5. P. 354-385.
13. Michelle Frasher. *Data protection and the EU's anti-money laundering regulation*. November 23, 2021 / https://iapp.org/news/a/data-protection-and-the-eus-anti-money-laundering-regulation/
14. Milaj J., Kaiser C. 'Retention of data in the new Anti-money laundering directive – 'need to know' versus 'nice to know''. *International Data Privacy Law*, 2017. Vol. 7 (2), p. 115-125. https://academic-oup-com.skaitykla.mruni.eu/idpl/article/7/2/115/3106233.
15. Parfitt N. 'AML Compliance – Data Privacy challenges'. *Risk & Compliance*, July 2019. Pages 2-5.

https://www.acurisriskintelligence.com/assets/RC_JUL19%20REPRINT_ACURIS_AML.PDF

16. Pavlidis G. 'Financial information in the context of anti-money laundering: broadening the access of law enforcement and facilitating information exchanges'. *Journal of money laundering control*, 2020, Vol.23 (2), p. 369-378. https://www-emerald-com.skaitykla.mruni.eu/insight/content/doi/10.1108/JMLC-10-2019-0081/full/html
17. Pfisterer M. V. 'The right to privacy – a fundamental right in search of its identity: uncovering the CJEU's flawed concept of the right to privacy'. *German Law Journal*, Vol 20, Issue 5, July 2019, P. 722-733.
18. Pranevičienė B. 'Limiting of the right to privacy in the context of protection of national security'. SSN:1392-6195. *Jurisprudence: research papers.* Mykolo Romerio universitetas. Vilnius: 2011. Nr. 18(4), p. 1609-1622.
19. Pranevičienė B. 'Limiting of the right to privacy in the context of information technology development'. *Public security and public order: scientific articles* (6) / Mykolo Romerio universiteto Viešojo saugumo fakultetas. Kaunas: 2011. T. 6, p. 254-270.
20. Preciosi C. *Finding the balance between data protection and AML requirements*. June 23, 2017. https://www.lexology.com/library/detail.aspx?g=8aabfbf8-33c1-456d-869b-ef1f56ec0e08.
21. Shainski R. *For Banks, Data Privacy and Anti-Money Laundering Don't Have to Be Incompatible.* 2019. https://www.cpomagazine.com/data-privacy/for-banks-data-privacy-and-anti-money-laundering-dont-have-to-be-incompatible/.

OTHER SOURCES

1. Directorate General for Financial Stability, Financial Services and Capital Markets Union. Training for lawyers on anti-money laundering (AML) and counter terrorist financing (CFT) rules at EU level (2022 February 25), https://finance.ec.euroopa.eu/publications/training-lawyers-anti-money-laundering-aml-and-counter-terrorist-financing-ctf-rules-eu-level_en.
2. European Union Agency for Fundamental Rights and Council of Europe. Handbook on European data protection law: 2018 edition, https://fra.euroopa.eu/en/publication/2018/handbook-European-data-protection-law-2018-edition.
3. CJEU Fact sheet on protection of personal data (November 2021), https://curia.euroopa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf. Accessed 9 September 2022.

4. Directorate General for Justice and Consumers of the Commission. Stregthened EU rules to prevent money laundering and terrorism financing (Fact sheet) 9 July 2018, https://ec.euroopa.eu/newsroom/just/document.cfm?action=display&doc_id=48935. Accessed 9 September 2022.
5. EDPS Opinion of 2 February 2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC, Access to beneficial ownership information and data protection implications, https://edps.euroopa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf. Accessed 21 November 2022.
6. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). Anti-Money Laundering Measures and Counter-Financing of Terrorism: Lithuania (Fifth Round Mutual Evaluation Report, December 2018), https://rm.coe.int/committee-of-experts-on-the-evaluation-of-anti-money-laundering-measur/16809247ed. Accessed 14 October 2022.
7. 1st enhanced Follow-up report & Technical compliance re-rating on Anti-Money laundering and Counter terrorist financing measures (Lithuania) June 2020, https://www.fatf-gafi.org/media/fatf/documents/reports/fur/Moneyval-1st-Follow-Up-Report-Lithuania.pdf. Accessed 21 November 2022.
8. 2nd enhanced Follow-up report & Technical compliance re-rating on Anti-Money laundering and Counter terrorist financing measures (Lithuania) November 2021, https://www.fatf-gafi.org/media/fatf/documents/reports/fur/MONEYVAL-FUR-Lithuania-Nov-2021.pdf. Accessed 14 September 2022.
9. Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing (2020), https://www.fntt.lt/data/public/uploads/2020/05/final-nra_eng_v3.pdf. Accessed 16 October 2022.
10. https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed 21 November 2022.
11. https://aml-cft.net/library/predicate-offence/. Accessed 21 November 2022.
12. https://ec.euroopa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en#:~:text=It%20includes%20the%20collection%2C%20recording,or%20destruction%20of%20personal%20data. Accessed 23 November 2022.
13. https://www.goldinglawyers.com/what-is-smurfing-example-of-how-smurfing-differs-from-structuring/. Accessed 23 November 2022.
14. https://www.tookitaki.com/compliance_hub/shell-companies-money-laundering/. Accessed 21 November 2022.

15. https://www.15min.lt/verslas/naujiena/finansai/penkiais-adresai-iregistruota-7000-imoniu-15min-aplanke-ir-atradimai-sokiravo-662-1025250. Accessed 18 November 2022.
16. https://www.icas.com/professional-resources/anti-money-laundering-resources/latest-developments/aml-awareness-three-stages-of-money-laundering. Accessed 11 November 2022.
17. https://financialcrimeacademy.org/money-laundering-cryptocurrency/. Accessed 5 September 2022.
18. https://vdai.lrv.lt/lt/naujienos/automobiliu-nuomos-bendrovei-skirta-bauda-del-duomenu-saugumo-pazeidimo-pagal-bendraji-duomenu-apsaugos-reglamenta. Accessed 9 October 2022.
19. https://en.wikipedia.org/wiki/British_Airways_data_breach. Accessed 2 September 2022.
20. https://termly.io/resources/articles/biggest-gdpr-fines/#:~:text=breaking%20Amazon%20fine.-,1.,for%20Data%20Protection%20(NCDP). Accessed 9 October 2022.
21. https://www.reuters.com/technology/irish-regulator-fines-facebook-265-mln-euroos-over-privacy-breach-2022-11-28/ Accessed 28 November 2022.
22. https://www.fatf-gafi.org/about/historyofthefatf/. Accessed 7 September 2022.
23. https://www.investopedia.com/terms/a/aml.asp. Accessed 13 October 2022.
24. https://www.cfatf-gafic.org/documents/fatf-40r. Accessed 14 October 2022.
25. https://www.acams.org/en/resources/aml-glossary-of-terms#a-9799feca. Accessed 20 October 2022.
26. https://ec.euroopa.eu/newsroom/fisma/items/29693/en. Accessed 20 October 2022.
27. https://en.wikipedia.org/wiki/November_2015_Paris_attacks. Accessed 3 October 2022.
28. https://www.fntt.lt/en/money-laundering-prevention/activities/226. Accessed 11 October 2022.
29. https://www.fntt.lt/en/money-laundering-prevention/applied-measures-for-breaches-of-the-aml-cft-law/4169. Accessed 11 October 2022.
30. https://www.fntt.lt/lt/pinigu-plovimo-prevencija/fiktyviu-imoniu-veiklos-pozymiu-nustatymo-gaires/4112. Accessed 3 November 2022.
31. https://www.fntt.lt/en/money-laundering-prevention/legal-acts/legal-acts-of-the-republic-of-lithuania/347. Accessed 31 October 2022.
32. https://www.lb.lt/en/prevention-of-money-laundering-and-terrorist-financing. Accessed 31 October 2022.
33. https://amlcenter.lt/en/. Accessed 26 October 2022.
34. https://www.coe.int/en/web/moneyval. Accessed 26 October 2022.

35. https://www.imolin.org/. Accessed 29 September 2022.
36. https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2022.html. Accessed 27 September 2022.
37. https://euroasiangroup.org/en/fatf-style-regional-bodies#:~:text=Eight%20FATF%2Dstyle%20regional%20bodies,FATF%20Recommendations)%20throughout%20the%20world. Accessed 13 September 2022.
38. https://sherloc.unodc.org/cld/en/st/home.html. Assessed 5 October 2022.
39. https://www.idnow.io/glossary/amla-eu/. Accessed 11 November 2022.
40. https://www.mastercard.co.uk/en-gb/personal/find-a-card/general-prepaid-mastercard.html. Accessed 3 November 2022.
41. https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2022.html. Accessed 3 November 2022.
42. https://egmontgroup.org/. Accessed 11 November 2022.
43. https://www.coe.int/en/web/moneyval/jurisdictions. Accessed 16 November 2022.
44. https://scsanctions.un.org/9v1k8-en-dprk.html#alqaedaind. Accessed 21 November 2022.
45. https://www.sanctionsmap.eu/#/main. Accessed 18 November 2022.
46. https://sanctionscanner.com/blog/what-is-a-sanction-list-8. Accessed 16 November 2022.
47. https://www.oxfordlearnersdictionaries.com/definition/english/fairness#:~:text=the%20quality%20of%20treating%20people%20equally%20or%20in%20a%20way%20that%20is%20reasonable. Accessed 18 November 2022.

ABSTRACT

Despite being commonly recognized and fundamental, right to privacy is limited in cases of justifiable need and public interests. Then again, prevention and combatting of money laundering is a set of rules developed for societal safety and stability of financial networks. This paper is focused on analysis of two virtues, namely right to privacy and anti-money laundering procedures in respect to their collision points. By complying with AML requirements, obliged subjects inevitably process certain extent of personal data, irrelevant whether a consent or even an awareness of data subject is present. The research is helpful to build knowledge on legal bases under GDPR to process these data and legal conditions for justifiable interference into right to privacy of individuals involved in ML in any role.

Keywords: privacy, money laundering, anti-money laundering, interference into fundamental human right.

THE CONCEPT OF PRIVACY: LEGAL RESTRICTIONS ON PRIVACY IN THE CONTEXT OF MONEY LAUNDERING PREVENTION

SUMMARY

The research of this thesis aims to analyze the collision points of a fundamental human right to privacy and anti-money laundering measures. Both virtues are vital to individual and society at large but are contradictory in essence: the more privacy legal framework protects, the less effective fight for crimeless society becomes, as AML is resultative only when certain data are collected, used and shared with competent authorities for prevention and combat purposes.

In four chapters of the paper, investigation starts by addressing the concept of privacy and developing differences between privacy right and right to data protection. This brings to conclusion that a right to privacy is not absolute and can be interfered in some situations when certain obligatory conditions are met.

Then the research focus shifts to the concept of money laundering and its combatting measures. An excessive explanation as to historic backgrounds, legislation on EU level, AML related networks and content of ML activities are presented. As a result, ML appears to be a long-term multilayered criminal activity where a predicate offense is present and many participants, aware and unaware, are used in various stages of the crime.

Third part of the paper narrows the attention to main contact points in AML activities where any interference to privacy right is inevitable. Notably, personal data are collected, processed and shared on both internal and external levels and this adds to the legal puzzle an element of transferring personal data to third parties. Even in narrative, the occurence of limitations to individual privacy is found significant.

Research continues with analysis for reasoning on how and to what extent the interference to privacy right can be performed in AML area to become permissive and balanced with the limited right. The results of the investigation of this paper have shown, that legislation and case law acknowledged limitations on fundamental rights if they are lawful and justified and do not breach the essence of interfered right. In every case, justification is found by checking compliance of restrictive measure with principles of proportionality, necessity and certainty in definition. Moreover, AML relations have exclusive legal grounds for data processing during limitations of privacy rights, though key principles of data processing under GDPR must be maintained.

Both money laundering and anti-money laundering activities are ever evolving processes, with imminent concern on maintaining balance between sacrifices in scope of limitations to fundamental human rights and gains by safeguarding the society from financial crimes.