University of Groningen

Privacy and Identity Issues in Financial Transactions

Kaiser, Carolin

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

*Document Version*
Publisher's PDF, also known as Version of record

*Publication date:*
2018

Link to publication in University of Groningen/UMCG research database

*Citation for published version (APA):*
Kaiser, C. (2018). *Privacy and Identity Issues in Financial Transactions: The proportionality of the European anti-money laundering legislation*. University of Groningen.

**Copyright**
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment.

**Take-down policy**
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

*Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.*

Download date: 03-06-2022

# Privacy and Identity Issues in Financial Transactions

Carolin Kaiser

Colofon

ISBN print book: 978-94-034-0977-1
ISBN e-book: 978-94-034-0976-4

Cover design by Michel Cents.
Lay-out: Ferdinand van Nispen, Citroenvlinder DTP&Vormgeving, *my*-thesis.nl
Print: GVO drukkers & vormgevers, Ede, The Netherlands

university of groningen

# Privacy and Identity Issues in Financial Transactions

The Proportionality of the European Anti-Money Laundering Legislation

**PhD thesis**

to obtain the degree of PhD at the
University of Groningen
on the authority of the
Rector Magnificus Prof. E. Sterken
and in accordance with
the decision by the College of Deans.

This thesis will be defended in public on

Thursday 25 October 2018 at 14.30 hours

by

**Carolin Kaiser**
born on 19 May 1987
in Vechta, Germany

**Supervisors**
Prof. G.P. Mifsud Bonnici
Prof. J.A. Cannataci

**Assessment Committee**
Prof. N. Forgó
Prof. G. Sartor
Prof. O.O. Cherednychenko

*Für Irmgard Warschewski*

## Acknowledgements

There are many people to whom I am endlessly grateful for their help around and during this project. My parents, for supporting me without fail. Katharina, Uwe, Carsten, and Christoph for offering shoulders and arms whenever needed (and they were often needed). Esgo for attentively listening to long-winded explanations of minute details that never even made it into the book. Gosha and Fiore for emotional support in the last phases of the project.

A special thank you goes to my colleagues at the University. Especially to Jeanne and Joe for endless support during the project. To Jonida for open ears and an open mind for any wild idea I came up with. Martin, Aukje, and Nicolas Cage for perfect sunday evenings. Matthijs, Gerard, and Peter for extraordinary lunches. Catherine, Saleh, and Oskar for motivational speeches. Nynke and Karen for sunshine. And all other colleagues who have made these four years so enjoyable and successful: Laurence, Karien, Hans, Styliana, Nati, Mel, Trix, Warscha, Rick, Lorenzo, Dimitry, Evgeny, Barend, and Björn.

Finally, special thanks to Michel Cents for designing the cover of this book.

## Overview

# Table of Contents

# Chapter I

## Introduction

## Outline:

a. The Areas of Research
   i. Outlining the Anti-money laundering Framework
   ii. Identity, Privacy, and Data Protection
   iii. Introducing Alternative Systems for Financial Transactions
b. Research Questions
c. Scope
d. Sources and Methodology
e. Outline and Logic of the Chosen Structure

## a. The Areas of Research

### i. Outlining the Anti-money laundering Framework

"Of evils current upon earth the worst is money", wrote *Sophocles* resignedly.[1] Many may still agree with this axiomatic statement almost 2,500 years after it was thus made. Indeed, a large segment of our legal system is concerned with counteracting this evil. This segment in particular contains numerous laws and rules designed to prevent people from benefitting financially from committing crimes. Prominent among these laws is the Anti-money laundering Directive (4AMLD) 2015/849.[2]

The crime of money laundering has undergone a rapid, nearly unprecedented development as a criminal offence in Europe.[3] Introduced throughout Europe in the late eighties of the last century to early 2000's,[4] it is a rather new offence compared to most other offences found in the national criminal codes of the Member States of the European Union. Money laundering is a crime that is difficult to define in general terms, due to the variety of strategies that can be used to launder money. In simple terms, money laundering is the act of concealing the origin of funds derived from criminal activity in such a way, that those funds can be used without raising suspicions regarding their provenance. Money laundering is in principle a logical step after any crime generating a material benefit to the perpetrator, which is why the volume of funds laundered in Europe is estimated to be extremely high.[5]

The approach chosen by the European legislator in the Anti-money laundering Directive is based on the global standards of anti-money laundering, developed and integrated in collaboration between a large number of states, international organisations, and expert groups. The approach is to oblige all financial services providers as well as other professionals, such as lawyers, real estate agents, and

1 *Creon* in Sophocles, Antigone (1962), p. 337.

2 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117.

3 Warde (2007), p. 240.

4 See for instance Arzt (1990), p. 1 f; Tracfin annual report 2015, p. 82; Oerlemans et al. (2016), p. 37.

5 The United Nations Office on Drugs and Crime (no date) estimates that the amount of money laundered each year corresponds to ca. 2-5% of the global GDP. This currently amounts to up to ca. 2 trillion USD. See also Hetzer (2002), p. 413.

gambling services providers, to comply with a quadrant of obligations: In the first place, all such obliged parties must identify each individual customer.[6] The aim of this measure is to create transparency by fully identifying each party to a transaction. Secondly, all transactions must be monitored by the obliged party to filter out any transactions that raise suspicions of money laundering or terrorist financing.[7] Whenever such a suspicion is raised, the obliged party must thirdly report this transaction to the competent authorities.[8] Fourthly, even in the absence of any suspicion, all records must be kept by the obliged party for a period of five years after the end of the business relationship with the customer.[9] The sum of those measures is meant to create a situation in which indicators of financial crime are identified by private service providers and then delivered to the authorities. The authorities should then be in a position to follow the paper trail of those transactions to uncover the operation and all persons involved,[10] and to base their case against the offender on the information collected and retained by financial services providers.

It should be stated at the outset, however, that the viability of this chosen approach is disputed, as the continually increasing extent of anti-money laundering measures, in both scope and severity, is so far not rewarded by any measurable success,[11] neither in the shape of a decrease of the volume of funds laundered, nor in the shape of an increase of the number of successful investigations of money laundering or terrorist financing.[12] This lack of success is one of the main reasons why the global standards for anti-money laundering are continually in motion and under review.[13] This continual motion is, in turn, reflected by a rapid change on a European level, with two amendments to the anti-money laundering legislation in quick succession.[14]

6 Article 11 juncto article 13 (1) (a) and (b) 4AMLD.
7 Article 13 (1) (d) 4AMLD. The legal text uses the more neutral term 'monitoring'. See also Stalla-Bourdillon (2013), p. 704.
8 Article 33 4AMLD.
9 Article 40 (1) 4AMLD.
10 Reimer/Wilhelm (2008), p. 240.
11 As shown for instance in Nestler/Herzog, Geldwäschegesetz, 2. Aufl. 2014, § 261 StGB, Rn. 17 ff.
12 FIU Jahresbericht 2016, p. 17.
13 Shasky Calvery (2013), p. 53.
14 COM (2016) 450, p. 2 f. The fourth Anti-money laundering Directive was passed in 2015, and the fifth Anti-money laundering Directive was proposed in 2016.

**ii. Identity, Privacy and Data Protection**

Naturally, an approach so focused on the comprehensive identification of customers, the surveillance of transactions, and the retention of data, raises concerns when contrasted with the interest of individuals in the protection of their identities and their privacy. The data processing operations prescribed by the Directive are immense. Particularly the surveillance these measures entail is a concern. Surveillance, in this context, can be defined as "institutionalised intrusions into privacy",[15] meaning that the large-scale intrusions into the privacy of individuals under surveillance becomes a rule rather than an exception. Examining the compatibility of such surveillance with the rights to privacy and data protection is the core task pursued by this thesis.

The rights to privacy and data protection are internationally recognised human rights. These rights are, among other documents, enshrined in the Charter of Fundamental Rights in the European Union (the Charter), and in the European Convention of Human Rights (the ECHR). It lies in the nature of the rights to data protection and privacy that they are engaged in every data processing operation, and it equally lies in the nature of the anti-money laundering measures that data processing is at the core of the approach taken against these offences. The compatibility of the anti-money laundering measures with human rights must therefore be examined carefully to ensure that human rights are duly respected in the design of the framework.

The rights to data protection and privacy are not absolute. They can be limited to a certain extent whenever an act of processing meets the conditions for a lawful interference with these rights.[16] The principle of proportionality is one of the conditions for an intrusion into the rights to privacy and data protection, and simultaneously a marker for the outside limit of the lawful extent for such an intrusion. This principle must be respected in every limitation of a human right.[17] According to the principle of proportionality, very simply put, an interference with the rights to privacy and data protection is lawful only when the interference occurs in pursuit of a legitimate objective in the public interest, for the achievement of which an encroachment upon those rights is requisite, and when the interference is limited to what is strictly necessary in order to achieve this objective.[18]

15 Schwartz (1968), p. 742. See also Leith (2006), p. 111; Westin (1984), p. 70 f.
16 Article 52 of the Charter; article 8 (2) ECHR.
17 See also Leith (2006), p. 111; early Holaind (1899), p. 151 ff.
18 Barak (2013), p. 251 ff.

Of particular note is also the low amount of discourse on the identity issues connected to the anti-money laundering measures. The Directive not only demands that every customer must be identified, but also that anonymous accounts and passbooks are prohibited.[19] The proposed fifth Anti-money laundering Directive is expected to limit options for anonymous transactions even further.[20] This lack of options for anonymity in financial transactions is deplorable from the perspective of privacy, as such options are best suited to ensure the protection of the identity, privacy, and personal data of individuals.

Indeed, the connection between anti-money laundering measures and the rights to privacy and data protection has so far not received the attention it deserves. Very little literature examines the compatibility of the measures with human rights in any detail.[21] Indeed, the rights to privacy and data protection are often brushed aside with few comments in an examination of the anti-money laundering framework.[22] This is due partly to the fact that, firstly, the fight against money laundering and terrorist financing is perceived to be of paramount importance.[23] Secondly, the limited literature may be a symptom of a general lack of recognition of the importance of the link between anti-money laundering and the rights to privacy and data protection.[24] Indeed, legislators appear to be largely unaware of it,[25] or perhaps unwilling to dig into the subject matter.[26] Simultaneously, while the anti-money laundering measures have been, and are being, designed on an international level with global integration, the rights to privacy and data protection are not yet recognised uniformly throughout the world. Indeed, even in Europe these rights are relatively new compared to other human rights, and legislation and case law are still in a process of early development. It is the ambition of this thesis to contribute to the discourse and development of this field of law.

19 Article 10 (1) 4AMLD.
20 Schaar (2016).
21 Leslie (2014), p. 264 ff.; Schaar (2016). See Wright/Friedewald/Gellert (2015), p. 45, who attest to a lack of attention to the right to privacy on the European level in general.
22 See for instance FATF information sharing (2016), p. 27.
23 COM (2016) 450, p. 2 f.
24 FATF information sharing (2016), p. 27.
25 See, for instance, the Commission's statements on the proportionality of the measures of the fourth Anti-money laundering Directive COM (2016) 450, p. 6 f., or the statements of the Polish government concerning indefinite retention periods, in General Secretariat of the Council, 15615/16, p. 2. In all of these documents, measures constituting intrusions into privacy are discussed, but a discussion of safeguards or proportionality is either entirely absent or very short and incomplete.
26 The reasons for the absence of in-depth discussions of privacy in official documents connected to the Anti-money laundering Directive can only be guessed. It may be speculated that regulators on the European and national levels are simply trying to avoid a difficult discussion.

### iii. Introducing Alternative Systems for Financial Transactions

The anti-money laundering measures are designed for efficient and comprehensive application by the banking sector and other financial services providers. The majority of the European population is covered by the dense network of banking services provided by an interplay of banks, credit card companies, transaction services, and payments systems of various kinds, offline and online. These are all part of the mainstream financial sector, and thus referred to as the "conventional banking sector" for the purposes of this thesis. There are, however, also financial transactions systems that lie outside of this mainstream network, and serve a niche. Two of those are virtual currency systems and the Hawala network.

Virtual currency systems are slowly struggling towards mainstream acceptance, but are as yet a novel phenomenon, both for society at large and for the lawmaker and regulators.[27] Virtual currencies are defined in the draft of the fifth Anti-money laundering Directive as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically".[28] This definition is rather vague because it must cover a variety of virtual currencies in circulation, which can differ to a large extent in various points.

The type of virtual currencies that are to be examined here primarily are decentrally organised. There is thus no central authority through which all transactions are routed as there would be in a bank;[29] instead, the users are connected via a peer-to-peer network. On this network, the units are exchanged among the users directly rather than with the intervention of a central authority.[30] The transactions are furthermore all recorded in a central ledger, called blockchain. By recording all transactions ever carried out through the system, the ledger allows the system to take account of all existing units. Users can refer to it to verify that the other party to a transaction in fact possesses the means necessary for the transaction, a task which would otherwise be carried out by a central authority.[31] The main example for such a decentrally organised virtual currency is Bitcoin, but the description

27 Luther (2016), p. 401 f.
28 COM (2016) 450, draft article 3 (18), p. 30. See also Bonaiuti (2016), p. 36; Vardi (2016) p. 59 f.
29 Raman (2013), p. 68; Rückert (2016), p. 14 f.; Hildner (2016), p. 486 f.
30 Shasky Calvery (2013), p. 56; Simmchen (2017), p. 163.
31 Allaire (2013), p. 115 f.

given above also fits a large number of other virtual currencies, which have been designed based on the same principles as Bitcoin.[32]

Virtual currencies hold great potential in the market of financial services, which is being recognized by a growing number of users and businesses.[33] However, the architecture of the system is entirely decentral, without any official representation, kept up by a number of people simply running a computer programme. Also, as the system operates online, these people are strewn all over the globe. Therefore, European legislation is ill-equipped to cover this network.[34] The geographic scope of any piece of European legislation is of course limited to the territory of the Member States, but many members of the system are based in third countries and therefore not covered by European legislation. In addition, any individual out of the group of people running the code and administering the system can hardly be considered to be offering financial services, which will remove the system itself from the personal scope of anti-money laundering legislation. What remains within the scope of the Directive are businesses established within the territory of the European Union, who offer services connecting to the virtual currency environment, such as online shops, gambling services, and online currency exchanges.

Operating decentrally and without a business at its core, a virtual currency can provide cheap, fast, and secure transactions, is attractive as an investment or for speculation, and convenient for use in legitimate and illegitimate online transactions.[35] In addition, the lack of a central authority applying anti-money laundering obligations also means that users are not covered by the monitoring carried out by financial services providers under the Anti-money laundering Directive. While the blockchain is publicly accessible to other users as well as law enforcement authorities, it is much harder to monitor than transactions in a bank. This makes virtual currencies attractive for users legitimately seeking such privacy, but it makes virtual currencies also attractive vehicles for tax evasion, the sale and purchase of illegal goods and services, and money laundering.[36]

32 Nakamoto (2008), p. 2 f. See also Hildner (2016), p. 487.
33 Raman (2013), p. 70.
34 Lowery (2013), p. 77.
35 Raman (2013), p. 68; Hildner (2016), p. 487.
36 Shasky Calvery (2013), p. 55; Murck (2013), p. 96 f.; Rückert (2016), p. 6.

Virtual currencies are not the only alternative transactions systems outside of the conventional banking sector, however. A second example for a transaction system that falls outside of the conventional regulated web of financial services providers are systems like Hawala.[37] In contrast to virtual currency systems, the Hawala system operates almost exclusively in the physical world, by basing its services on cash. The Hawala system is in principle a network of individuals (hawaladars) providing financial transactions as a service to their community. A much simplified example can serve to explain the service. When a customer approaches a hawaladar to send a certain sum of money to a recipient in a different city, the hawaladar contacts a colleague in that city and asks him to pay that sum out to the recipient. The sender pays the hawaladar in cash, and the hawaladar's colleague pays cash to the recipient. The cash does not, however, move physically. Instead, next time the cash flow may be reversed, and the hawaladar's colleague may ask the hawaladar to pay out a certain sum to a recipient. If the value of the transactions coincide, the second transaction balances the books and removes the imbalance created by the first transaction.

Moving value without moving physical cash is a very fast and safe means for transaction, which is provided in a very similar way by the conventional banking sector through online banking services. Especially the simplicity of the service attracts customers. Hawala thrives in many countries in Asia and the Middle East, and is thus often more familiar to members of the expatriate community from those countries in Europe than the conventional banking system.[38] Furthermore, it is fast, cheap, private, secure, Sharia compliant, and reliably reaches remote and rural villages, areas of violent conflicts, and countries subject to embargoes and capital controls. At the same time, these factors which can be advantages to legitimate customers, can also be advantages to illegitimate customers wishing to move funds covertly. The Hawala system is thus vulnerable to abuse for money laundering and terrorist financing operations, tax evasion, and other restricted transactions.[39]

37 There are numerous systems operating similarly to Hawala, but Hawala was chosen as their representative for the purposes of this thesis, as information on it was most accessible to the author. See also Chapter III (e) below for information on this choice, and FATF Hawala (2013). This FATF report was an important source.
38 Marin (2009), p. 918 f.
39 See also Collins (2005), p. 86 f.

Regulators on the European and national level have a very difficult task in reaching out to hawaladars for compliance with rules covering other providers for financial transactions.[40] Awareness of this system within the general population is low, as Hawala systems are often almost exclusively provided by a member of a certain expatriate community to other members of the same community. Furthermore, compliance with the financial regulations faced by providers of financial services is very costly, which is one reason why many hawaladars may prefer to dispense with their obligations, and choose instead to risk paying a fine for operating an unlicensed business if their business activity is noticed. hawaladars often operate in an environment in which the customers' identities are personally known to them,[41] but the frequent lack of compliance by hawaladars with financial regulations makes it possible for a customer to use the services of a hawaladar in the confidence that the transaction will remain hidden.

Therefore, both systems are potentially vulnerable to abuse for money laundering operations. The incomplete coverage of the systems by anti-money laundering measures perhaps makes them more attractive for financial crime and money laundering. This vulnerability has been recognised, and the relationship between anti-money laundering rules and alternative systems is subject to much debate on the different venues on which the anti-money laundering framework is calibrated.[42] However, both the Hawala systems and virtual currencies are well-known only to small segments of society. On the level of regulators, they both appear to be viewed generally with suspicion,[43] and the interest in properly protecting legitimate users is largely disregarded.[44]

## b. Research Questions

The Research Problem addressed in this thesis is the connection the between three different but closely connected themes outlined in the previous section. In the first place, there is the anti-money laundering legislation. This legislation must secondly be in accord with human rights, and in particular with the concepts

40 See for more details Chapter III section (e) below.
41 Razavy/Haggerty (2009), p. 148.
42 COM (2016) 450, p. 12 f.
43 Murck (2013), p. 101; Luther (2016), p. 401 f.
44 See, however, Shasky Calvery (2013), p. 56, whose statements are an exception to the rule.

of identity, privacy, and data protection. Thirdly, the connection between the foregoing two is stirred by alternative transactions systems, which not only challenge the traditional categories of the anti-money laundering framework, but also the protection of financial data. The intersection between these three themes is the area of research of this thesis.

The overarching main research question is whether the anti-money laundering measures as currently applied across Europe properly respect the rights to privacy and data protection. According to article 52 of the Charter of Fundamental Rights of the European Union, a measure is in accord with human rights only if it is provided for by law, respects the essence of the right, and if the intensity of the interference of the measure with human rights is necessary and proportionate to the aim it pursues.[45] The principle of proportionality is often the crux of the test, and will therefore serve as a yardstick by which the respect for human rights of the anti-money laundering measures is to be reviewed.

This main question concerning the respect for human rights of the anti-money laundering framework is best answered by first considering a network of related sub-questions. The first sub-questions concern the background of the anti-money laundering framework and alternative transactions systems: What measures does the anti-money laundering framework consist of? After analysing the anti-money laundering measures, alternative transactions systems can be introduced. The two primary preliminary questions concerning alternative transactions systems are firstly, what they are and how they function, and secondly, if and how they are covered by the anti-money laundering framework.

A second set of sub-questions follows. This set assists in building the theoretical framework within which the main research question is to be answered. The first question concerns the rights to privacy and data protection: What is the content of these rights? This concerns especially the proper protection of these rights as the assessment of their protection is an integral part of the main research question. Secondly, the concept of identity will be discussed, due to its close connection to the measures which are to be discussed.[46] It adds another facet to the discussion

45 See, for example, CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, paragraph 38.

46 Two of the main measures of the Anti-money laundering Directive, which will be discussed in detail in the following chapters, is that all customers of an obliged entity must be identified, and that anonymous instruments are nearly entirely prohibited.

of privacy and data protection. Sub-questions relevant in this context are, what is the content of the two concepts of identity and anonymity, and how do those concepts relate to privacy and data protection? Finally, prefacing the answer to the main research question, the principle of proportionality must be examined in detail. This principle already been mentioned several times, but what precisely is the content of the principle of proportionality as applied by the CJEU and ECtHR, and how has it evolved over the course of recent case law?

Once those sub-questions are answered, the main research question will be in full focus. The third set of sub-questions concerns the evaluation of the anti-money laundering measures and cumulatively serve to conclusively answer the main research question. In what ways, if any, do these measures interfere with the rights to privacy and data protection? Do the measures pursue a legitimate aim? What are the concerns that the anti-money laundering measures raise, particularly in terms of privacy and identity, and particularly in the light of the latest case law of the CJEU? And finally again the main research question: Do the anti-money laundering measures as currently applied in Europe properly respect the rights to privacy and data protection?

The impact of the outcome of the proportionality assessment should also be considered: What are the consequences of a decision that the Directive is disproportionate? Also, could alternative transactions systems perhaps offer enhanced protection to users, in order to shield them from disproportionate interference?

## c. Scope

The close connection of this thesis to European law is evident in the research questions. The main focus of this thesis lies on the measures contained in the Anti-money laundering Directive (EU) 2015/849. However, the measures prescribed in this Directive are neither unique nor original.[47] Anti-money laundering is an extremely international field of law, with a large number of global, European, and national instruments interconnecting to make up a quickly evolving and ever growing framework. This network has generated a global standard for

47 Sorel (2003), p. 374.

anti-money laundering law, consisting of a series of recommended measures and approaches, which are applied in a rather similar fashion in many different jurisdictions across the globe. A representative legal instrument was chosen in order to limit and substantiate the scope of this examination. The choice here fell on the fourth Anti-money laundering Directive 2015/849,[48] as one of the latest legal instruments in this area, and one of the most influential, as it will to a large extent govern the anti-money laundering policy of the Member States. In addition, despite the fourth Anti-money laundering Directive being so new, it is already under review at the time of writing, and a fifth Anti-money laundering Directive is expected to introduce relatively minor changes to the framework shortly. The latest developments concerning this legal amendment are also considered.

The Financial Action Task Force (FATF) guidelines were also consulted frequently, as the Directive explicitly refers to them several times, citing the need to update the European framework to bring it into accordance with the FATF's newest Recommendations.[49] The standards set by the FATF are therefore an important source for the interpretation of the Directive. However, not only did the FATF guidelines influence the European legislator, the European Commission and several Member States were directly involved in shaping the FATF Recommendations.[50] In sum, the European Anti-money laundering Directive was chosen as a representative of the global standard of anti-money laundering measures, but due to the global and cohesive nature of the anti-money laundering system, findings based on an examination of this particular Directive can be applied to many other laws and instruments in the field of anti-money laundering.

The stated intention of this research is to assess whether the anti-money laundering framework is compatible with the human rights standard in the field of privacy and data protection. The instrument that is to be evaluated is a European directive,

48 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117.

49 See Recitals 3, 4, 11, 28, 33, 43, and 44, and Annex II (3) (d) to Directive (EU) 2015/849.

50 The FATF is one of the most important global fora for anti-money laundering and countering the financing of terrorism with 37 Member jurisdictions, one of which is the European Commission itself. Of the other 36, 15 are European Member States, and five are other states located on the European continent. See also Chapter II (d) below.

and it must then, as all European directives, adhere to the standards by which the compliance of directives with human rights is measured.[51] On the one hand, this concerns the human rights guarantees of the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights. Both of these instruments contain sections on privacy and data protection, which are very much interconnected and interrelated. On the other hand, and closely related to the former, this concerns the principle of proportionality. This principle is not only one of the most important principles in European law, but it also to a large extent governs the application of the human rights guarantees[52] in the Charter and the ECHR.[53] A discussion of other human rights instruments is largely omitted, in order to sharpen the focus and to be able to go into the more detail concerning those instruments.

Generally speaking, the human rights guarantees contained in the Charter are applied by the Court of Justice of the European Union, and the human rights guarantees contained in the ECHR are applied by the European Court of Human Rights. The two courts do, however, closely follow and reference one another's decisions and findings. Both courts also apply a similar proportionality test.[54] Therefore, the case law of these two courts is essential for understanding the substantial content of the rights to privacy and data protection and the principle of proportionality. While other courts, particularly national constitutional courts, also play a very important role in the application of the principle of proportionality, and especially in ensuring the abidance by human rights, the focus has been laid on the case law of the ECtHR and the CJEU. The reason is their evident strong connection to the two human rights documents that are to be applied. In particular, the data retention case law of the CJEU is authoritative due to the close connection between the Data retention Directive and the Anti-money laundering Directive. In addition, the concrete anti-money laundering measures contained in the Directive are to be tested, and the CJEU is exclusively competent to assess whether a directive properly respects human rights and the principle of proportionality

51 See also Aaken (2009), p. 487 f.

52 The right to non-discrimination, the rule of law, the presumption of innocence, and the freedom to conduct a business also play a role in the final assessment of the terms of the Directive. See also for instance the fourth, sixth, seventh, and eleventh concerns discussed in Chapter IX below.

53 See, for instance, CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, paragraph 38.

54 See for details Chapter VIII below.

(article 5, 6 TEU). The case law of the ECtHR is used to supplement the case law of the CJEU, because the Charter builds upon the ECHR, and because the CJEU in its judgments frequently refers to the case law of the ECtHR, emphasising the connection of the two documents and courts in questions of human rights.

This dual approach to human rights documents and case law will be supplemented in the final chapters of this thesis, in which a judgment of the German Constitutional Court is brought into the analysis of the proportionality of the anti-money laundering measures in addition to the case law of the two European courts. This is due to the fact that the German Constitutional Court in its influential judgment on data retention expanded on several points which are relevant to the question of proportionality and can therefore supplement the discussion. In addition, the Court in its decision made several interesting observations on the nature of the rights to privacy and data protection, which allows an analysis beyond the current line of case law taken by the European courts, and beyond the letter of the human rights documents that are to be consulted here. These observations are to be taken up in more detail in Chapter X of this thesis.

Finally, the scope is defined by the choice of transactions systems that are examined. There are numerous different systems that can be used to carry out a financial transaction. Three groups of transactions systems will be examined. In the first place, the conventional banking system is used as a basis for comparison. The conventional banking system comprises numerous different institutions and companies, but the primary representative here chosen for this banking system is a bank in which private persons may keep a personal bank account. The conventional banking system is also the system for which the anti-money laundering measures in their current shape and form have been principally designed. Besides the conventional banking system, there are numerous alternative systems that can be used.[55] The choice fell on two alternative systems, to stand as representatives for the many different systems in existence. In the first place, the Hawala system was chosen to represent the large variety of informal transfer systems.[56] It was chosen because it is the largest and most comprehensively studied system, and extensively used among the immigrant communities around Europe. In the second place, Bitcoin will stand as a representative for the many different virtual currencies

55 Anderson (2014), p. 429.
56 See for the hazy distinction between formal and informal remittance providers IMF (2005), p. 10.

now in existence. It is the original virtual currency, and to date still the biggest, although the virtual currency scene is rapidly evolving. Limiting the scope of the research in this way allows a deeper consideration of these systems, while findings can be applied to the majority of alternative systems not individually studied here.

## d. Sources and Methodology

The main sources for this research are legal texts, literature and case law. In the first place, the text of the laws themselves, particularly the network of Directives and the Charter and the ECHR, were of course the most important primary sources. In addition, the official documents recording the genesis of the law were also considered, supplementing the interpretation of the law. Furthermore, the output of authorities on the European level was considered, particularly of the European Data Protection Supervisor and of the Article 29 Working Party. Other secondary literature was gathered from many different sources, with academic articles naturally making up the biggest share of the reading. Furthermore, articles in both English and German language were considered, with a few excursions into French and Dutch language publications. In addition to academic articles, the financial and the technology news were followed closely over the course of the project, in order to stay on top of the rapid developments pertaining to the area of research. Particularly the amendments to the anti-money laundering legislation and the development of virtual currencies was covered extensively in the news media, the latter with significantly more popular coverage and attention than the former. References to Hawala in the media were few and far between.

Once the decision was made to limit the scope of the research to a sharply focussed discussion on the European level, it followed that the case law was also largely to be limited to the case law of the Court of Justice of the European Union and the European Court of Human Rights. Relevant case law of the highest national courts was, however, read and considered as far as possible in order to be sure that interesting leads and new developments were not missed. Only one national case became integrally relevant to the research, however, due to exhibiting such an interesting lead.[57]

57 This was the German Constitutional Court's assessment of the data retention legislation, BVerfG, 1 BvR 256/08 [2010].

In addition, a close albeit informal connection to the communities of users of the Hawala and virtual currency systems has been kept up, in order to better learn about and understand both systems, and in order to avoid falling prey to any of the common misconceptions about the systems and their users. Common misconceptions concerned in particular how the two systems worked and why they are chosen by a user. For instance, numerous publications incorrectly refer to virtual currencies as being anonymous,[58] and others insist on linking Hawala directly to terrorism.[59] Others concerned the culture predominant in the two systems, particularly the use of dark web marketplaces for the sale of drugs in virtual currencies[60] and religious aspects in Hawala,[61] both of which are correct connections, but certainly not the sole pillars on which the importance of each of the systems rests. These prejudices are connected to the culture in which the use of these systems is embedded, which cannot conclusively be learned from the scholarly consideration of paper sources. However, it should be emphasised that the contact with users of alternative transactions systems was not intended to serve as a source for information, but rather in order to verify statements made in academic literature. This is due to the legal rather than sociological focus of this thesis, and due to the fact that some contacts indicated that they would have been unwilling to share information in a formal setting.

The above paragraphs outline the existing knowledge upon which the present research is built. This research aims to add a new facet to the existing literature, by combining the topics of anti-money laundering and privacy, a line of research which has not yet been explored in depth. It also adds to the growing body of literature on blockchain and virtual currencies by discussing the privacy perspective of the regulation of virtual currencies. The literature on all of the topics which are tied into this research, namely anti-money laundering, privacy, identity, and alternative transaction systems, are in various stages of development, but certainly not exhaustively studied and described in literature.

58 Prominently the European Commission in the original proposal for the fifth Anti-money laundering Directive, COM (2016) 450, draft Recital 7 (p. 22); Anderson (2014), p. 433. See also Raman (2013), p. 66.

59 See for instance Schramm/Taube (2002), who in the title of their publication call Hawala "al Quaida's Global Financial System" or Jamwal (2002), who calls Hawala "The Invisible Financing System of Terrorism".

60 The take-down of the market place *Silk Road* has generated enormous attention and has occasioned a hearing in the United States Senate in 2013, see Carper (2013), p. 2 f.; Carr (2003), p. 193 f.

61 See Razavi (2005), p. 281 for a sober analysis of the connection between Hawala and Islam.

The innovation brought by this thesis is the combination of the fields of research, which are seldomly combined in this way. While the upcoming fifth Anti-money laundering Directive is connecting virtual currencies to anti-money laundering measures, this connection has hardly been studied in the existing literature. As has already been mentioned above, the aspect of privacy in this connection does not receive adequate attention in literature or in the official documents connected to the law-making procedure. The results of the assessment carried out in this thesis are therefore a unique addition to the state of the legal literature. Similarly, this thesis will ask some rather difficult questions about the principle of proportionality in Chapter X. While there is a beginning of a constructive discussion of these questions in German literature, there are at this moment no voices participating in such a debate on the European level. This thesis aims at making the beginning of such a debate.

Based on the research of the sources and due to the subject matter, the topic is approached in different manners in the individual chapters. In the first place, there are necessarily several descriptive elements, in order to map out the problem and in order to give sufficient background information to readers not familiar with certain aspects of the topic, and in order to answer the relevant sub-questions of the research. This concerns for instance the details of the different financial transactions systems, charted in Chapter III. In addition, the divergence of the different components of the topic, particularly technical details, made it very likely that a reader would not be familiar with all of the different aspects of the research, making an accessible simple language highly desirable.

In the second place, it should be emphasised that a functional approach to the law was applied wherever possible.[62] In very simple terms, under the functional theory of law, the black letter of the law is not considered alone; instead, the effect of the law is researched, considered, and used to supplement the study of the letter of the law.[63] This consideration of the effect of a law is particularly indispensable when considering the impact of a legal measure on the human rights of an individual. The functional method falls into several different schools, several of which have been used in this research. In this way, the case law has been analysed following a pragmatic approach,[64] considering the development of the case law of the different

62 See also Kielmansegg Graf (2008), p. 24.
63 Cohen (1935), p. 826.
64 See also application by Solove (2002), p. 1090 ff.

courts in context with the evolution of the law and in view of the potential future developments of the jurisprudence. Close attention to the development of the jurisprudence is particularly important in the discussion of the rights to privacy and data protection as well as in the assessment of the proportionality principle, which have been formed significantly by jurisprudence. This concerns particularly Chapters V and VIII of this thesis. Complementing this approach, the realistic school has also been followed in the assessment of the case law, in order to trace the development of the case law. In the words of *Cohen*, "a judicial decision is an intersection of social forces: Behind the decision are social forces that play upon it to give it a resultant momentum and direction; beyond the decision are human activities affected by it."[65] This realistic view is particularly important in considering the (potential) impact of the case law, and is therefore exceptionally useful in the transfer of existing lines of case law to slightly different legal questions. Such a transfer was undertaken in order to answer the main research question in Chapter IX.

In the third place, interdisciplinary research was carried out, adding elements particularly of sociology and political science in selected sections in order to complete a picture of the texture of the problem not easily settled in law alone.[66] A deeper dive into these social sciences as well as computer science and cryptology was omitted in view of the scope and in the interest of the consistency of the research. However, particularly research into social sciences is directly connected to the realistic approach as outlined above.[67] Interdisciplinary research has been undertaken especially in the drafting of Chapters III, VI, and VII, which all combine elements of legal science with the various relevant neighbouring disciplines.[68]

Finally, conclusions have been reached by deconstructing the elements of the anti-money laundering framework, analysing them in detail, and then applying a normative evaluation to these elements, following the theory of rational balancing.[69] In particular, *Duncan Kennedy's* work on the Hermeneutics of Suspicion[70] was influential in the assessment and normative evaluation of the legal rules in question, especially in the proportionality assessment carried out in Chapter

65 Cohen (1935), p. 843. See also Nelson (1920), p. 1 ff.
66 See also Leith (2006), p. 106; Pound (1922), p. 18 ff.
67 See also Jellinek (1914), p. 82 ff.
68 See in this context also Jellinek (1914), p. 27 ff.
69 See Aaken (2009), p. 503 f.
70 Kennedy (2014), p. 102 ff.

IX. In this context, the relevant case law is also taken apart into the individual elements of the cases in order to connect them to the measures in question. A critical view of these elements was then taken, in conformity with the view *Cohen* stated so concisely: "We never shall thoroughly understand the facts as they are, and we are not likely to make much progress towards such understanding unless we at the same time bring into play a critical theory of values."[71] The evaluation was furthermore guided by the human rights-based approach, placing the human rights to privacy and data protection into the centre of the inquiry.[72] This approach can be traced particularly in the final Chapters IX and X.

## e. Outline and Logic of the chosen structure

This thesis is split into three parts of roughly equal length and import. The first part, comprising Chapters II, III, and IV, deals with setting the scene in which the research questions can be answered, explaining the background in terms of the law and in terms of the instruments to be examined. The second part, comprising Chapters V, VI, VII, and VIII, details the theoretical framework, explaining the concepts of privacy and identity against which the measures of the anti-money laundering framework are to be tested. The final part of the thesis, Chapters IX and X, is the evaluation, in which the examination of the measures and a normative discussion is to take place.

The first part begins with Chapter II, in which the elements of anti-money laundering legislation are delineated. Not all readers will be intimately familiar with the details of the fourth and fifth Anti-money laundering Directives of the European Union. The details of these Directives are, however, the substance of the following assessment, and must therefore be discussed in minute detail in Chapter II at the very beginning of the inquiry.

In the following Chapter III, alternative transactions systems are then described and explained in detail. In the past few years, awareness of alternative systems of financial transactions has increased in the general population. Some readers may have heard of Hawala in connection with the financing of terrorism in the

71 Cohen (1935), p. 848 f. See also Taylor (2017), p. 400 f.
72 See also *Paulsen* in Hinneberg (ed.) (1908), p. 283 ff.

months and years following the events of September 11th, 2001, although even then, meaningful and unagitated coverage of the system was scarce. Similarly, the general population is increasingly aware of virtual currencies, first sparked by media coverage of the take-down of the market place for illegal goods Silk Road[73] and the prosecution of its operator, but more and more also of innovative business models based on a virtual currency itself, or on the underlying technology of the blockchain, as well as investment options in virtual currencies. However, both systems are to most people only known by name, without a clear concept of the underlying system. Therefore, a detailed explanation of each of these system is indispensable to ensure that readers previously unfamiliar with the two systems are acquainted with the details of each system before applying legal concepts to them. Chapter III is dedicated to this explanation.

The following Chapter IV contains an examination of how each of the two alternative systems is covered by the anti-money laundering framework. While the third Anti-money laundering Directive was in force during most of the period of research, the fourth Anti-money laundering Directive was passed in May 2015, and entered into force in June 2017, and therefore, the measures of this fourth Directive are primarily analysed here. A fifth Anti-money laundering Directive is already underway, however. In July 2016, the Commission has formally proposed an update to the fourth Directive. This proposal is relevant in particular concerning its explicit inclusion of virtual currencies into the scope of the Directive, which is why it is being included into the assessment, but only punctually, as the text has not been formally adopted at the time of writing. This concludes the first Part on the Background.

The second part of this thesis concerns the framework of interpretation. This begins with Chapter V, in which the details of privacy and data protection are mapped out. A discussion of the compatibility of the rules of the Anti-money laundering Directive with those rights makes it necessary to preface such a discussion with a detailed introduction of the content of the European privacy framework. Chapter V therefore introduces the rights to privacy and data protection in the shape they take in the Charter of Fundamental Rights of the European Union, as well as in

73 Shasky Calvery (2013), p.53 f.; Dowd (2014), p. 70 ff.; Van Houten/Bingham (2014), p. 186 f.

the General Data Protection Regulation (GDPR)[74] and the Police and Criminal Justice Authorities Directive,[75] although the national legal systems are at the time of writing still in the process of being updated to accommodate the GDPR and the implementation of the Directive.

In the following chapters, two points are going to be highlighted in order to complete the framework of this thesis, which are the complexes of identity in Chapter VI, and of anonymity and pseudonymity in Chapter VII. The concept of identity is of particular interest in several ways. Identity is intimately connected to the concept of personal data.[76] Data is only protected as personal data under the GDPR when it relates to an identified or identifiable person.[77] At the same time, the Regulation also refers to less clearly defined concepts such as the cultural and social identity of a person.[78] A person's cultural identity is often decisive in his or her choice for a transaction system such as Hawala. In addition, one of the three major duties of all entities obliged under the Anti-money laundering Directive is to identify each and every customer. The concept of identity is therefore a core concept which ties the two fields of anti-money laundering law and privacy together.

Similarly, anonymity and pseudonymity are important connecting factors between those two areas. As personal data must relate to an identified or identifiable person, the removal of this relation through anonymization largely removes data from the scope of the GDPR. For such an important function, however, guidance on anonymity and pseudonymity is scarce in the legal texts. Therefore, the first sections of Chapter VII are devoted to clearing the misconceptions and ambiguities about both terms. Following such elucidation, the two main appearances of the concept of anonymity in law are analysed. Those are firstly the aforementioned GDPR, where anonymity may be a way to comply with the principles of data minimization, or for data subjects to ensure a high level of protection of their data, and secondly the

74 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 [GDPR]) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

75 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

76 See Reiman (1984), p. 314; Gavison (1984), p. 351.

77 See also Durner (2006), p. 214.

78 Article 4 (1) GDPR.

Anti-money laundering Directive, which summarily forbids anonymous accounts or passbooks.[79] Anonymity is, however, a particularly effective way for individuals to protect their privacy and identity, and should therefore be a desirable option in conformity with the principle of data minimisation.[80] The concept of anonymity furthermore also connects to the two alternative systems for financial transactions in that customers are generally not as rigorously identified and monitored when using those systems as when using the conventional banking sector.

In the following chapter, Chapter VIII, a detailed discussion of the principle of proportionality will follow. Chapter VIII is intimately connected to the previous chapters, particularly Chapter V on privacy and data protection, because in order to fill the proportionality standard with meaning, the case law of the CJEU and the ECtHR is discussed, examining the evolution of the principle of proportionality as applied by these two Courts in their case law on the rights to privacy and data protection. This chapter furthermore serves as a basis for the evaluation of the proportionality of the anti-money laundering measures, which is to take place in the following chapter. Chapter VIII concludes the second Part of this thesis.

The final third Part on the Evaluation begins with Chapter IX, concerning an analysis of the legality of the Anti-money laundering Directive, based on the issues identified in previous chapters. In Chapter IX, the proportionality of the measures prescribed by the Directive is to be assessed. The assessment is based principally on the judgments of the CJEU on data retention measures. In its judgment of 8 April 2014, the CJEU invalidated the Data retention Directive for disproportional interference with the rights to privacy and data protection. In a following judgment of 21 December 2016, the Court had the opportunity to repeat, clarify, and extend its findings of its previous judgment, reprehending national data retention laws. The lessons distilled from this case law in connection with the comments on proportionality made in Chapter VIII can also be applied to the anti-money laundering framework. While the subject matter of the decisions serving as a theoretical framework concern communications data rather than financial data, the Data retention Directive presents some striking similarities to the Anti-money laundering Directive, and the judgments are constructed in such a way that they lend themselves very well for translation to the Anti-money laundering Directive.

79 Article 10 (1) of Directive (EU) 2015/849.
80 Article 5 (1) (c) of the GDPR; Schantz (2016), p. 1842; Richter (2016a), p. 92.

In addition to the three judgments of the CJEU, a judgment of the German Constitutional Court (*Bundesverfassungsgericht*, BVerfG) is also used in this assessment. The CJEU's invalidation of the Data retention Directive[81] was predated and followed by a large number of national judgments on data retention, for which this judgment by the BVerfG may serve as an example. In its judgment of 2 March 2010, the BVerfG ruled the German national law on data retention to be unconstitutional. This judgment is interesting in several ways. The BVerfG is a court of exceptionally good reputation, and it can be assumed that the CJEU was well acquainted with the content of this judgment when composing its own decision less than two years later. Evidence of this influence can be found in the wording of the CJEU's judgment, which is in some passages very similar to that of the BVerfG. Furthermore, the BVerfG devotes much more space to its evaluation of the data retention measures than the CJEU, delivering interesting material insights and considerations missing from the leaner text of the CJEU's judgment. The main research question will be answered in Chapter IX.

Chapter X therefore follows after the main research question was already answered. It could be considered as an epilogue to this thesis, the outline of a viable approach to mass surveillance in the future, and a guidepost towards a line of research that shall be pursued elsewhere. It connects to the judgment of the BVerfG, which was not only selected as a supplement to the case law of the CJEU and ECtHR to support the assessment carried out in Chapter IX. The judgment also contains one highly interesting and widely discussed remark, in which the Court reprimands the German lawmaker for its excessive intrusions into the privacy of the population through mass surveillance. The Court in its decision outlines an obligation on the lawmaker to carefully survey the full range of surveillance measures already in place when considering to adopt a further measure, in order to determine whether an additional surveillance measure can be tolerated by society. The idea is that a free and democratic society can only absorb a certain level of surveillance before it loses the traits free and democratic due to excessive control,[82] and that only a careful observation of all measures with which society is already burdened can prevent this loss of freedom and democracy.

81 Leutheusser-Schnarrenberger (2014), p. 590 f.
82 See also Hohmann-Dennhardt (2006), p. 547; Tinnefeld (2007), p. 628; Maras (2012), p. 72.

This idea appears worthy of some remarks which will conclude this thesis. It can be translated to the European level by connecting it to the lawmaker's duty to respect the essence of the right to privacy when introducing limitations to this right. The essence of a human right is a concept which has not yet received material elaboration by the CJEU. However, German constitutional law can again be referred to. Article 19 (2) of the German constitution also forbids intrusions into the essence of the human rights established by the constitution. Just as the discussion of the judgment on data retention of the CJEU is supplemented by the influential earlier decision of the BVerfG, the discussion of the concept of the essence of privacy protected in the Charter is to be supplemented by the influential constitutional tradition of article 19 of the German Constitution. It is to be argued, therefore, that based on the particular importance of the right to privacy for a free and democratic society, the concept of the essence of this right must be fleshed out to a holistic approach as suggested by the BVerfG. Chapter X of this thesis is devoted to a short discussion of this notion.

Finally, this thesis ends with the Conclusion (Chapter XI). That chapter contains a summary of the main findings of this thesis and six conclusions which may be drawn. Each of the conclusions is connected to a number of recommendations. The recommendations are not only addressed to one certain group of readers, but may be aimed at regulators on the European or national level, obliged entities, NGOs, or the general public, depending on the content of the recommendation in question. The conclusion is rounded off by an overview of recent and ongoing developments in the field of research, and finally highlights a number of questions related to this thesis, which demand further research.

To sum up, this thesis begins its first part with a detailed explanation of the anti-money laundering framework (Chapter II) and of alternative systems for financial transactions (Chapter III), followed by a discussion of the application of the law to those systems (Chapter IV). The following second part of the thesis on the theoretical framework begins with a discussion of the rights to privacy and data protection (Chapter V). A detailed discussion of the two concepts of identity (Chapter VI) and anonymity and pseudonymity (Chapter VII) follows. The second part of this thesis ends with an analysis of the case law of the CJEU and the ECtHR in order to define the elusive principle of proportionality (Chapter VIII). Based on the foregoing, the third part on the Evaluation is begun with the examination of

the proportionality of the Anti-money laundering Directive (Chapter IX). Finally, a holistic approach to the essence of privacy is outlined (Chapter X) in order to perhaps strengthen the protection of the rights to privacy and data protection in the future. Results are summarised in Chapter XI.

# PART A

# THE BACKGROUND: FINANCIAL SERVICES, MONEY LAUNDERING, AND TERRORIST FINANCING

# Chapter II

## Understanding the Anti-money laundering Framework

## Outline:

a. Introduction
b. Money Laundering
    i. Definition and Stages of Money Laundering
    ii. Property
    iii. Predicate Offences
c. Terrorist Financing
    i. Definition
    ii. Funds
d. Background: International Cooperation
    i. Early Efforts: the United States
    ii. The Financial Action Task Force
    iii. Developments in Europe
    iv. The Patriot Act
    v. International Efforts to Combat Terrorist Financing
    vi. Recent Developments in Europe
e. The Fourth Anti-Money Laundering Directive 2015/849
    i. Obliged Entities
    ii. Financial Intelligence Units
    iii. Obligations
        (1) Identification of Customers
        (2) Surveillance of Transactions
        (3) Reporting of Suspicious Transactions
        (4) Record Keeping
    iv. Risk Assessments
f. Ongoing Developments
    i. The Proposed Fifth Anti-Money Laundering Directive
    ii. Terrorist Financing
g. Critique
    i. The Anti-money Laundering Approach
    ii. The Approach Taken against Terrorist Financing
    iii. Lack of Data Protection Safeguards
    iv. Concerns
h. Conclusion

## a. Introduction

It is not easy[83] to hide the details of one's finances, particularly finances connected to an illegitimate source of wealth, from the authorities. This concerns especially the tax authorities if said illegitimate wealth is tucked away out of their sight,[84] and the criminal justice authorities if this illegitimate wealth is derived from a criminal enterprise. If one wishes to use these funds, it is necessary to explain the origin of valuable property in order to keep the suspicions of the authorities averted from one's untaxed deposit or criminal enterprises. This is where money laundering is undertaken.

The laundering of 'dirty money' is necessary in order to be able to carry on one's criminal activity undisturbed and at the same time to enjoy the fruits of one's labour. It can also come into play when hidden untaxed funds are to be brought back from obscurity safely, without raising questions on the part of the tax authorities concerning their origin. Money laundering is essentially the act of concealing the illicit origins of funds in order to make them appear legitimate. Anti-money laundering measures are the corresponding measures that are taken to prevent the illicit origins of any property from being concealed, and to prevent perpetrators of crime to benefit from this criminal activity.[85]

Since the early 2000's, the measures originally put into place to combat money laundering have also been applied to terrorist financing.[86] Terrorist financing is the act of providing a terrorist enterprise with a material benefit of any kind. Terrorist financing is similar to money laundering in that both activities involve the covert movement of property. However, while in money laundering the origin of funds must be concealed, a terrorist financing operation must conceal their destination. At the same time, money laundering necessarily involves a crime at its beginning, while the funds displaced for the purposes of terrorist financing are generally intended for the financing of a potential future terrorist attack,[87] or simply the ordinary day-to-day expenses of a terrorist group.

83 The difficulty of this undertaking varies and may be assessed differently by different people. Some of the factors making money laundering easier or more difficult are discussed at various points in this chapter.
84 Kaetzler (2008), p. 180.
85 Köllner/Mück (2017), p. 593; Trüg (2017), p. 1913.
86 Golden et al. (2011), p. 514; Warde (2007), p. 240 f.
87 Sorel (2003), p. 378; Sotiriadis/Heimerdinger (2009), p. 234.

This chapter is dedicated to the detailed discussion of both the phenomena of money laundering and terrorist financing and the applicable anti-money laundering framework currently in place in Europe. The most important and latest items within this regulatory framework are of course the fourth Anti-money laundering Directive (EU) 2015/849,[88] and the proposed fifth Anti-money laundering Directive, which is at the time of writing still in the process of the law-making procedure.[89] These two Directives are, however, only the newest links in a long chain of directives, recommendations, and a network of international conventions and recommendations concerning this topic. In order to create a more complete picture of the background of the fourth Anti-money laundering Directive, its history and international integration is also to be outlined briefly.

A detailed discussion of the anti-money laundering measures is naturally indispensable at the beginning of this thesis. Considering that the main research question concerns the compatibility of these measures with human rights, it is necessary to ensure that the reader is familiar with the existing framework at the outset,[90] and to shed light on the individual measures and their development. This chapter is on the one hand going to give a sober, technical account of the framework in order to provide a good basis for, on the other hand, an analysis of the anti-money laundering measures. A normative judgment will be made in Chapter IX. The remarks made in this chapter are of great importance for all following chapters, as they provide minute details on the anti-money laundering measures which are discussed over the course of this thesis, and may be referred back to whenever needed.

This chapter begins a discussion of the anti-money laundering measures, which is going to be continued in Chapter IV, where the application of the measures of the Anti-money laundering Directive on alternative transaction systems is going to be

88 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117.

89 Procedure 2016/0208/COD: COM (2016) 450: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 Directive 2009/101/EC.

90 The discussion of the human rights in question will take place in Chapter V below.

discussed. After the theoretical framework was built in Chapters V, VI, VII, and VIII, Chapter IX will take up all of the leads begun in this chapter and continue the analysis of the anti-money laundering measures.



This chapter begins with an explanation of what money laundering and terrorist financing are, in sections (b) and (c). Following this initial definition of the phenomena, the discussion will turn to instruments of anti-money laundering and combating the financing of terrorism. To set the existing measures into their historical context, section (d) is concerned with a short outline of the development of the anti-money laundering framework, before turning to a detailed discussion of their current organisation. Section (e) concerns the detailed discussion of all relevant measures contained in the fourth Anti-money laundering Directive, which fastens the current standard of anti-money laundering legislation in the European Union. Section (f) is furthermore concerned with looking ahead at developments currently ongoing, particularly changes to the framework to be brought about by the fifth Anti-money laundering Directive. Finally, section (g) is to outline the main points of critique commonly levelled against the approach chosen against money laundering and terrorist financing. It principally discusses the data protection provisions contained in the Anti-money laundering Directive, and begins to outline the discrepancies between the Directive and privacy and data protection.

## b Money Laundering

The introduction of anti-money laundering measures is supported by a number of different considerations. The European anti-money laundering Directives have always[91] reasoned that money laundering should be fought for its potentially negative effect on the financial system.[92] There are several other reasons to support an effective anti-money laundering approach. One main reason for the support of measures against money laundering is that criminals should not benefit from having committed a crime. This reason is certainly one which can be generally

91 The need to protect the integrity, stability, and soundness of the financial system was discussed in the first two recitals of 1AMLD already.
92 See recitals 1 and 2 4AMLD.

agreed on.[93] It is a principle applied often in criminal law that the material benefit of a crime is forfeit.[94] It is hoped that when crime is not economically advantageous, the number of incidents will decrease.[95] Therefore, the fight against money laundering is at the same time a fight against all crime: economic benefit is one of the main motives for commission of criminal activity, and one of the purposes of anti-money laundering is to ensure that the economic benefit of a given criminal offence becomes uncertain, and the crime itself therefore unattractive.

**i. Definition and Stages of Money Laundering**

The whole purpose of money laundering is to give dirty money a new legitimate story, i.e. to make funds derived from criminal activity appear legitimate. Money Laundering is generally carried out in three stages: Placement, Layering, and Integration. During the first stage, "money derived from criminal activities is introduced into the financial system."[96] Money laundering is thus always preceded by a predicate offence, criminal activity that has generated revenue. In small amounts, money needs not be laundered, as it could easily be explained away as being savings or a gift. In large amounts, it becomes more difficult to explain how these funds have come into one's possession. Therefore, particularly when cash is to be laundered, the very first step is often to divide large amounts of funds into small tranches and pay them into a number of accounts, preferably at different banks in different cities.[97] If it is possible, those different cities are also located in different countries, in order to obscure the trail further and to limit the availability of information accessible to law enforcement agencies. Due to difficulties in logistics, however, the first step of money laundering usually takes place within the same country in which the funds have been generated.[98]

93 It should be emphasised that although this thesis is criticising the anti-money laundering approach rather severely, this basic statement that no criminal should benefit from having committed a crime is of course supported by the author. It is the measures taken against money laundering, and the severity of these measures, which will be criticised at various points in this thesis.

94 See for instance recital 1 of Directive 2014/42/EU.

95 Recital 3 of Directive 2014/42/EU.

96 Jost/Sandhu (2000), p. 12. See also Golden et al. (2011), p. 513; Oerlemans et al. (2016), p. 46 f.

97 Sorel (2003), p. 375.

98 Sorel (2003), p. 375.

In layering, the second step, "the money launderer manipulates the illicit funds to make them appear as though they were derived from a legitimate source."[99] The money launderer thus attempts to place several layers between the criminal activity and the funds derived from this activity, in order to obscure the origin of the funds and to make them appear legitimate. This can be achieved in many different ways. A popular method of layering is to move the money between different accounts at different banks in different countries, in order to make it more difficult for investigators to follow the paper trail.[100] Complicated ownership constructions using convoluted shell companies, particularly including stations at offshore 'tax havens', can also be used in order to disguise the origins of property.

Finally, in the third stage, "the launderer invests in other assets, uses the funds to enjoy his ill-gotten gains or to continue to invest in additional illegal activities."[101] The funds are thus integrated into the economy and can be treated and used as if they were legitimate funds. This final stage is often accomplished in developing economies with low levels of oversight, "because they are less finicky and greedier for capital."[102] Moving those legitimate funds back to the perpetrator of the original predicate offence is then comparatively easy, as the property can now be made to appear to be legitimately theirs.

These three stages already hint at the immense variety of possible money laundering operations. This is the reason why, in legal terms, money laundering is defined very broadly. The definition included in article 1 (3) 4AMLD reads as follows:

> "For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:
>
> (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of that person's action;

99 Jost/Sandhu (2000), p. 12. See also Golden et al. (2011), p. 513.
100 Sorel (2003), p. 375. See also Oerlemans et al. (2016), p. 46 f.
101 Jost/Sandhu (2000), p. 12.
102 Sorel (2003), p. 375. See also Golden et al. (2011), p. 513; Vlcek (2015), p. 413 ff.

> (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
>
> (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
>
> (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c)."

This very broad definition of money laundering, kept largely unaltered since the first Anti-money laundering Directive (article 1, first indent 1AMLD), in essence covers every aspect of this offence, going much further than the colloquial concept of money laundering, which generally covers only the action of hiding the origin of property derived from criminal activity in order to make it appear legitimate, emphasising the stages of layering and integration.

This corresponds to the dictionary definition, which is "the process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions".[103] This concept of money laundering is essentially the activity described in article 1 (3) (a) and (b) 4AMLD. It describes the active and intentional concealment of property of an illegitimate origin.[104] However, the definition included in the Directive then goes further than this concept, by including also activity in which the element of active 'laundering'

103 Oxford English Dictionary, Third Edition 2010, s.v. "money laundering".
104 Walter (2009), p. 571 f.

is entirely absent, for example in the mere acquisition, possession or use of contaminated property, under article 1 (3) (c) 4AMLD.[105]



**ii. Property**

Besides the fact that the legal definition of money laundering also includes activity which might not coincide with the colloquial use of the concept of money laundering, there is a second discrepancy with the colloquial use of the term and the legal definition. This concerns the term 'money'.

It is important to note that money laundering does not only concern money as such. Instead, the legal text speaks of 'property', as can be seen in the definition of money laundering of article 1 (3) 4AMLD cited above. The Directive also defines the term property as follows: "'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets" (article 3 (3) 4AMLD). Clearly, this definition is extremely wide, intended to catch all possible forms of property that might be used for the purposes of money laundering. Corruption, for instance, is one of the crimes which is to be curbed by strict money laundering oversight. It also often involves property other than money, such as luxury goods, or non-monetary advantages. All of these may fall under the definition of 'property', ensuring that loopholes are closed as far as possible.

**iii. Predicate Offences**

Money, or rather funds and property, only needs to be laundered if it is derived from a criminal offence, if the criminal activity from which the property was derived can be classified as a *predicate offence* for money laundering.[106] Which criminal activities are covered in principle depends on the national criminal legislation, but in article 3 (4) 4AMLD, the European legislator clarifies that

105 See also Walter (2009), p. 571 f. Note that the mere possession of contaminated property already falls under the definition of money laundering. This very wide definition of money laundering raises questions regarding the principle of *ne bis in idem* where, for instance, theft is the predicate offence. In the great majority of cases, theft is accomplished by bringing the item in question into the possession of the thief; it is therefore in the majority of cases impossible for a thief to commit theft without also committing money laundering. This question of the compatibility of the definition of money laundering with the principle of *ne bis in idem* is one objection which may be raised against the Directive. The seventeen concerns discussed in Chapter IX only focus on concerns connected to the data protection and privacy aspects of the anti-money laundering measures. This focus may inadvertently conceal the fact that the terms of the Directive are also problematic when viewed from other angles.

106 Walter (2009), p. 571 f.; Dittrich/Trinkaus (1998), p. 346.

"'criminal activity' means any kind of criminal involvement in the commission of the following serious crimes:

(a) acts set out in Articles 1 to 4 of Framework decision 2002/475/JHA;[107]

(b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;[108]

(c) the activities of criminal organizations as defined in Article 1 of Council Joint Action 98/733/JHA;[109]

(d) fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests;[110]

(e) corruption;

(f) all offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months".

107 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3–7. Footnote added by the author.

108 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted by the United Nations Conference for the Adoption of a Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, held at Vienna from 25 November to 20 December 1988, Registration No. 27627, UN Treaty Series vol. 1582, p. 95. Footnote added by the author.

109 Joint action 98/733/JHA of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union, OJ L 351, 29.12.1998, p. 1–3. Footnote added by the author.

110 Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the protection of the European Communities' financial interests, OJ C 316, 27.11.1995, p. 49–57. Footnote added by the author.

The list of possible predicate offences given by the European lawmaker requires some clarification. To begin with, point (a) refers to the criminal activity listed in articles 1-4 of Framework Decision 2002/475/JHA. The offences mentioned in article 1 (1) (i) of the Decision are terrorist offences, very broadly defined to include all imaginable manners of committing terrorist offences, as well as the threat to commit such offences. Article 2 of the Framework Decision includes leading and/or participating in a terrorist group, article 3 lists three offences committed as preparatory acts to committing a terrorist attack, and article 4 includes inciting, aiding, abetting and attempting any of the crimes listed in the previous three articles.

In the second place, article 3 (4) (b) 4AMLD refers to the offences listed in article 3 (1) of the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988. The Convention pledges its members to include the offences listed in this article in the national criminal codes. The offences listed in that article are manifold. They cover the production, transport, distribution, sale, purchase, possession, and all related activities pertaining to illegal drugs and other substances (article 3 (1) (i-iii) of the Convention). Furthermore, article 3 (1) (iv) of the Convention includes the manufacture, transport and distribution of equipment or material to be used in the production of any of these substances. Finally, the "organization, management or financing of any of the offences enumerated in i), ii), iii), or iv) above" is likewise to be a criminal offence (article 3 (1) (v) of the Convention).

Thirdly, article 3 (4) (c) 4AMLD points to Council Joint Action 98/733/JHA of 21 December 1998. The purpose of this Action, is, as its title says, "making it a criminal offence to participate in a criminal organisation in the Member States of the European Union". Article 1 of this Action defines a criminal organization as

> "a structured association, established over a period of time, of more than two persons, acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty, whether such offences are an end in themselves or a means of obtaining material benefits and, where appropriate, of improperly influencing the operation of public authorities".

Fourthly, article 3 (4) points (d) and (e) 4AMLD refer more generally to the protection of the financial interests of the Community and to the prevention of corruption. The inclusion of tax crimes in point (f) is closing a lacuna left in the third Anti-money laundering Directive 2005/60/EC.[111]

Finally, article 3 (4) (f) 4AMLD is a catch-all provision intended to leave no serious crime exempted from the list of predicate offences. The penal codes of the different Member States are organized according to different principles, depending on the tradition in which the code was drafted. They also reflect how serious a certain offence is considered by society in how severely it is punished.[112] Thus, for some offences, usually those which are not seen as the most serious of crimes, a maximum prison term is prescribed, and the judge has the discretion to award a shorter term, or, if applicable, forms of punishment other than imprisonment. For the second category of more serious crimes, a minimum prison sentence is prescribed, and the judge may award a longer sentence, but not a shorter term. So point (f) declares all the following crimes to be possible predicate offences for money laundering: in the first place, crimes on which a maximum sentence is fixed, if that maximum sentence is more than one year, or, in the second place, crimes on which a minimum sentence is fixed, if that minimum is more than six months. That the crimes must be serious enough to be punishable by a prison term of a certain amount is a way to ensure that only crimes of a certain gravity are included in the list of predicate offences to money laundering. This threshold should be strictly observed in order to prevent minor offences to be included and the meaning of the term 'serious crimes' to be watered down.[113]

Crimes which are, according to the first system, punishable by imprisonment of no more than one year, or, under the second system, punishable by six months or less, can thus be exempted from the range of predicate offences, and laundering funds derived from these crimes is not money laundering within the meaning of

111 See in this context also European Economic and Social Committee 13666/16, p. 4. The EESC urges that the efforts to combat tax crimes in the fourth Anti-money laundering Directive are not going far enough, and should be strengthened with the introduction of the fifth Directive. See also Kaetzler (2008), p. 180.

112 Note that the EESC urges harmonization of the legal treatment of those crimes on a European level, see European Economic and Social Committee 13666/16, p. 4.

113 It should be noted that Article 2 of the UN Convention against Transnational Organized Crime defines 'serious crime' as an offence that is punishable by a prison term of at least four years.

this definition. This exemption, however, does not apply to the crimes mentioned in points (a) to (e) of article 3 (4) 4AMLD. Any crime falling under points (a) to (e) are predicate offences in any case, regardless of how high or low the punishment in the national jurisdiction is set.

Article 3 (4) (f) 4AMLD thus very broadly includes any crime, irrespective of the plausibility of its being used for money laundering, as a possible predicate offence.[114] The difficulty in this regard is that even crimes with no obvious connection to money or property are included automatically under the provision. For instance, the punishment for battery, libel and slander, and environmental crimes will likely be of such a magnitude that they fulfil the conditions of point (f), but in the most cases, those crimes will lack a financial component leading to money laundering. Also, point (f) is intended to catch serious crimes, and it is perhaps debatable,[115] whether crimes such as libel and slander can truly be considered serious crimes.

## c. Terrorist Financing

The fight against terrorist financing has only been pursued on a large scale and internationally since the events of September 11th, 2001.[116] It is generally recognised that keeping up a terrorist group, maintaining the necessary infrastructure, and carrying out terrorist attacks, are rather costly undertakings. Therefore, the idea is that where the flow of finances to support the terrorist group is interrupted, it becomes more difficult to carry out terrorist attacks.[117] Financial constraints may therefore lead to a situation in which fewer terrorist attacks are carried out, and in which those attacks which could not be prevented are at least smaller in scale. At the same time, where the measures against terrorist financing help detecting the flow of funds, monitoring such a flow may lead to information on planned terrorist activity, and therefore potentially help preventing attacks.

114 Dittrich/Trinkaus (1998), p. 346. See also Frasher (2016), p. 32.
115 See also the sections on serious crimes in Chapter IX (f) below, where this point will be further discussed.
116 See Section (d) below for details of the development of an international strategy against terrorist financing.
117 Ryder (2007), p. 822 ff.

### i. Definition

The measures originally developed to be taken against money laundering are now also applied in the fight against terrorist financing,[118] and the anti-money laundering legislation generally covers these two distinct concepts together. Compared to money laundering, however, terrorist financing is a crime which inspires much more sinister associations and descriptions using martial terms and a strong Manichean rhetoric of good and evil:[119]

> "The financing of terrorism is a subterranean universe governed by secrecy, subterfuge, and criminal endeavors; but also a good measure of sophistication and an understanding of the global financial system. It is best described as [an] octopus with tentacles spreading across vast territories as well as across a wide range of religious, social, economic and political realities."[120]

Less dramatically put, terrorist financing is essentially simply the act of knowingly providing funding to terrorist organisations. The reasoning behind the criminalisation of terrorist financing is the idea that maintaining a terrorist organisation, recruiting new members, and carrying out attacks is costly, and that the removal of the funds used for such activity would result in a sharp decrease in attacks.[121] The Commission words it as follows:

> "Terrorist organisations and individual terrorists need financing – to maintain their networks, to recruit and supply, and to commit terrorist acts themselves. Cutting off sources of finance, making it harder to escape detection when using these funds, and using any information from the financing process to best effect can all therefore make a powerful contribution to the fight against terrorism."[122]

Terrorist financing occurs in as many different ways as money laundering does. One channel which has received a lot of attention is the abuse of non-profit organisations and (religious) charities for the purposes of moving funds particularly from Europe and North America to terrorist cells based in the Middle

118 Roberge (2007), p. 197 f.
119 Warde (2007), p. 243.
120 Raphaeli (2003), p. 59.
121 Lavalle (2000), p. 492.
122 COM (2016) 50 final, p. 2.

East.[123] In this context, it must be noted that "accurate evidence of charitable donations being used by terrorist groups is extremely rare."[124]

Also criminal activity on a small scale up to serious organised crime has been used to fuel terrorist activity, as in the case of ISIS, which has financially supported itself among other activity by "bank looting, extortion, control of oil fields and refineries, robbery of economic assets, kidnapping for ransom, cash smuggling[125] and grass-roots funding."[126] Note that some of these activities might be classified as terrorist acts in their own right, generating more funds for the financing of terrorism.



Article 1 (5) of Directive (EU) 2015/849 contains a short definition of terrorist financing. According to that article,

> "'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA".[127]

The definition of terrorist financing thus also refers to Council Framework Decision 2002/475/JHA,[128] just as point (a) of the definition of money laundering does, as was explained above. In the context of terrorist financing, these offences should be explained in more detail. Article 1 lists a number of offences, "which, given their nature or context, may seriously damage a country or an international organisation", with the subjective element of the intention being any of the following: "seriously intimidating a population, or unduly compelling a Government or

123 COM (2016) 50 final, p. 12. See also Sorel (2003), p. 373 f.; Ryder (2007), p. 825; Raphaeli (2003), p. 62 f.

124 Ryder (2007), p. 834.

125 See also FATF physical transportation of cash (2015), p. 27 ff. Footnote added by the author.

126 COM (2016) 50 final, p. 12. See also recital 13 of Directive (EU) 2017/541.

127 This definition in essence coincides with the definition of terrorist financing in article 11 of Directive (EU) 2017/541. See also Sorel (2003), p. 373.

128 Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3–7, since replaced by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21.

international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation". The offences are specified in detail in article 1 (1) (a-h) of the Decision, covering a large range of offences, from assault over hijacking of airplanes to the acquisition of nuclear weapons, as well as the threat to commit any of the offences listed in points (a) to (h) (article 1 (1) (i) 2002/475/JHA).

Article 2 of the same Decision defines the offences relating to the participation in terrorist groups. For this purpose, the article begins by defining the term 'terrorist group' in article 2 (1) 2002/475/JHA as

> "a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. 'Structured group' shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure".

Article 2 (2) of the Decision more specifically demands that the leadership of such a group, as well as the participation in such a group in any way, is punishable by law in all Member States.[129]

Article 3 of the Decision mentions 'terrorist-linked offences', which are theft, extortion, and forgery of documents, with the view of committing one of the offences listed in article 1 of the Decision. Finally, article 4 of that Decision includes inciting, aiding, abetting, and attempting any of the offences listed in the previous three articles.

To sum up, in principle, it can be said that money laundering is the act of veiling the criminal origins of property, while terrorist financing is the act of concealing the criminal destination of funds or property. The methods employed are often very similar, while the direction of the flow of the funds is the opposite.[130] In addition, the proceeds of criminal activities can of course be used in the financing of terrorist

129 Sotiriadis/Heimerdinger (2009), p. 235.
130 Sotiriadis/Heimerdinger (2009), p. 234.

activity.[131] This connection is one of the reasons why the fight against terrorist finance was added to the objectives of the anti-money laundering legislation.[132]

**ii. Funds**

Just as with money laundering, which does not necessarily involve money, terrorist financing also does not necessarily involve finances. Instead, the Directive speaks of 'funds'. It does not, however, include a legal definition of the term. Such a definition can be found in the glossary attached to the Financial Action Task Force (FATF) Recommendations, which, as will be seen below,[133] are essentially a blueprint for the terms of the European Anti-money laundering Directive. According to that source, "The term funds refers to assets of any kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments of any form, including electronic or digital, evidencing title to, or interest in, such assets."[134]

This definition coincides with the definition of property contained in the Directive. As is the case with money laundering, assets other than money can be used in terrorist financing operations. The intention behind this very wide definition is then again the interest in including all material advantages that might be rendered a terrorist operation in the definition of terrorist financing, to ensure that no loopholes remain.[135]

## d. Background: International Cooperation

At the outset, it is important to note that the anti-money laundering measures here discussed are not a European invention. In fact, the development of anti-money laundering rules is a process driven by a multitude of governments and international organisations, the European Union being only one actor among many, albeit a powerful and innovative one. The integration of international and European instruments was already seen above, when it was shown that the definition of the term 'funds' as used in the Anti-money laundering Directive is

131 COM (2016) 50 final, p. 9.
132 COM (2016) 50 final, p. 2.
133 In section (e) of this Chapter below.
134 FATF Recommendations (2012), p. 118; Ryder (2007), p. 821; Lavalle (2000), p. 496.
135 Lavalle (2000), p. 497.

found in the FATF Recommendations. Before going into the details concerning anti-money laundering measures, the international context and development of anti-money laundering law should therefore be discussed briefly.

It should be noted that there are so many instruments concerning anti-money laundering and the combat of terrorist financing on the international and even European level that it would go far beyond the scope of this thesis to discuss or even mention each item individually. Therefore, it was chosen to limit the scope of this chapter to only a few documents. Those are in the first place the United States Banking Secrecy Act of 1970 and the United States Right to Financial Privacy Act of 1978, as they illustrate the development of the modern anti-money laundering framework in its early stages, and secondly the USA Patriot Act of 2001, with which the framework against money laundering and the financing of terrorism were immensely extended. The approaches of which have found their way through international instruments into European law. The leading international player in this context is the Financial Action Task Force, whose Recommendations are generally seen as the global standard of anti-money laundering law[136] and will therefore flow into the discussion as well.

The discussion of other instruments had to be largely omitted. Therefore, despite their evident importance to the system as a whole,[137] the network of UN and COE Conventions, the output of expert groups such as the Egmont Group and Moneyval, the role played by Interpol and Europol in anti-money laundering, and other players and instruments in the field will not be discussed at this juncture. The reason for this omission is the repetitive content of the different international instruments,[138] their often non-binding character,[139] and because the standards contained therein often fall short of the FATF Recommendations and the Anti-money laundering Directives in both scope and detail. In particular, it should be noted that the succession of European Anti-money laundering Directives closely reflects, and significantly shapes the state of the art of international anti-money laundering measures.[140] This is caused by the rather frequent updates to the framework, and by the willingness

136 COM (2016) 450, p. 3. See also Sotiriadis/Heimerdinger (2009), p. 234.
137 Kaetzler (2008), p. 174; BMF (2004), p. 87.
138 Sorel (2003), p. 376; BMF (2004), p. 87.
139 See in this context also Liszt (1898), p. 4 f. for an early take on non-binding international instruments.
140 COM (2016) 450, p. 2 f.

of the Commission and Member States to make anti-money laundering and the combating of terrorist financing a policy priority.[141]



**i. Early Efforts: the United States**

Historically, the United States can be identified as the state that has taken the lead role in the fight against (international) money laundering operations.[142] One of the earliest examples of targeted legislation against money laundering can be found in the United States Bank Secrecy Act[143] of 1970. The most important innovation of that law was to establish a system of currency transaction reports, according to which obliged entities had to report any payment or transfer of value of more than 10 000 US Dollar.[144] Furthermore, this law set the basis for the strong emphasis on compliance in the financial sector, as the Bank Secrecy Act included detailed requirements as to the correct compliance with the measures introduced by it. Failure to comply with the reporting standard set by the Bank Secrecy Act was an issue for which the institution needed to assume strict liability.[145]

However, the rigid reporting threshold proved this law's greatest weakness. As *Gouvin* aptly observes: "As a general proposition, a substantial percentage of crooks who have more than $ 10,000 in cash to deposit are clever people; they quickly learned to make small deposits."[146] Another weakness of the Bank Secrecy Act was the inconsistent definition of obliged entities. The legislation was mainly aimed at banks and several other players in the financial sector besides, but led to a situation in which particularly financial transfer services were subject to less strict standards concerning record keeping than banks,[147] although their services are potentially very suitable for money laundering operations.

The lessons learned from the weaknesses of the Bank Secrecy Act have led to the development of the reporting of 'suspicious' transactions,[148] which is to prevent money laundering operations from remaining undetected simply for the fact that the value to be moved was one cent below a rigid threshold. The language currently utilized by the Anti-Money Laundering Directive, where it does resort

141 COM (2016) 450, p. 3 f.; FATF Money or Value Transfer Services (2016), p. 18.
142 Böszörmenyi/Schweighofer (2015), p. 64 f.
143 The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.), commonly referred to as Bank Secrecy Act.
144 Gouvin (2003), p. 963.
145 Gouvin (2003), p. 963.
146 Gouvin (2003), p. 964. See also Sorel (2003), p. 376.
147 Gouvin (2003), p. 964.
148 Gouvin (2003), p. 964.

to fixed thresholds, also includes "transactions which appear to be linked".[149] The threshold therefore also applies in cases where the value was split up into several transactions. Furthermore, the unequal treatment of some financial institutions and the subsequent abuse of those systems for money laundering operations led to the ongoing constant extension of the scope of the legislation and to an ever increasing number of obliged entities.

The idea that part of the fees paid by the customer to the financial institution for its services went toward covering the costs of the surveillance and reporting of the customer's transactions created some uneasiness among the customers.[150] This uneasiness led to a challenge of the Bank Secrecy Act before the United States Supreme Court, which, however, did not hold this act to be unconstitutional. The Supreme Court ruled that

> "There is no legitimate 'expectation of privacy' in the contents of the original checks and deposit slips, since the checks are not confidential communications, but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[151]

The Court therefore found that the Fourth Amendment to the United States Constitution, protecting citizens against unreasonable search and seizure, was not applicable in this case.

The Bank Secrecy Act was not, however, left in its original state for long. In 1978, the Right to Financial Privacy Act[152] was passed in order to counteract some of the negative effects of the Bank Secrecy Act, and to address the concerns of the customers of financial services. The main innovation of the Financial Privacy Act was to make the disclosure of financial records subject to the consent of the customer, if the customer was a private individual.[153] In practice, however, the level

149 For example in article 11 (b) (i) 4AMLD.
150 See, in this context, Schwartz (1968), p. 742.
151 Supreme Court of the United States, decision of April 21, 1976, *United States v. Miller*, 425 U.S. 435 (1976), pp. 441-443.
152 The Right to Financial Privacy Act of 1978 (12 U.S.C. ch. 35, § 3401 et seq.), commonly referred to as RFPA or Financial Privacy Act.
153 Gouvin (2003), p. 965.

of protection afforded by the Financial Privacy Act is watered down to the right of the customer of financial services to be notified prior to disclosure of personal information, and there were broad exceptions to this right, allowing for the delay of this notification by court order if such notice would potentially impede efforts of law enforcement authorities.[154]

Interestingly, this framework of anti-money laundering legislation was put into place long before money laundering itself was made a crime. The United States did not establish money laundering as a criminal offence until 1986, yet even at that time being one of the first countries worldwide to specifically criminalize this activity.[155] After this step, however, the United States led an international effort resulting the adoption of such statutes quickly all over the world.[156]

Throughout the 1990s, the money laundering rules were again amended several times. The first important change was to move from rigid reporting thresholds to the more flexible concept of suspicious transactions.[157] The 1992 amendment of the Bank Secrecy Act increased the reporting duties of the financial sector to implement this innovation, but the uncertainty of the definition of the concept of 'suspicious transaction' and the strict liability for failure to report (as opposed to the absence of liability for over-reporting)[158] caused a large amount of unnecessary reports, veritably drowning the authorities in paperwork and paralysing the administration.[159]

A second important notion of the 1990s was the first introduction of the Know Your Customer (KYC) approach.

> "The 1998 Know Your Customer proposal would have required financial institutions to determine the customer's identity, identify the source of customer funds, determine the customer's 'normal and expected'

154 Gouvin (2003), p. 966.
155 Leslie (2014), p. 169.
156 See for instance Arzt (1990), p. 1 f. for the adoption in Germany, Jong (2014), p. 25 ff. for the application of such rules in South Korea, Magrani (2014), p. 34 f. for the application in Brazil.
157 Gouvin (2003), p. 967.
158 Kaetzler (2008), p. 179; Dittrich/Trinkaus (1998), p. 344.
159 Gouvin (2003), p. 967 f. See also Ryder (2007), p. 836 f.; Lennon/Walker (2009), p. 41; Kaetzler (2008), p. 179.

> transactions, monitor accounts for transactions that were not consistent with those expectations, and determine whether such transactions were unusual or suspicious."[160]

However, this approach was at that time deemed to be much too far-reaching, and too much in conflict with the customers' rights. One might say that the measures were considered to be disproportionate.[161] The proposal was ultimately withdrawn and the act could not be passed at the time.[162]

**ii. The Financial Action Task Force**

Simultaneously to being developed domestically in the United States, the fight against money laundering was also further explored internationally. One of the recurring problems identified in anti-money laundering and in combatting of terrorist financing is the cross-border character of these crimes. Both terrorism and criminal activity show a propensity to involve several different countries at a time, and the laundering of proceeds of crime and the financing of terrorism also frequently connect several different jurisdictions.[163] The national character of most law enforcement operations leads to difficulties in the investigation into such cross-border movements, which indeed in turn makes international constructions more desirable for criminals. For this reason, close international cooperation in this field was soon recognised to be indispensable,[164] and an international organisation was brought into being, under which international cooperation in the field could be facilitated.

In this way, the Financial Action Task Force was established in order to facilitate a venue for such international cooperation concerned with the prevention and combating of (international) money laundering.[165] The FATF introduces itself as

> "an inter-governmental body established 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and

160 Gouvin (2003), p. 969; Zentes/Wybitul (2011), p. 92.
161 See for a detailed discussion of the proportionality of the terms of the fourth Anti-money laundering Directive Chapter IX below.
162 Gouvin (2005), p. 523.
163 COM (2016) 450, p. 14; Sorel (2003), p. 378; Kaetzler (2008), p. 174. See also Gordon/Morriss (2014), p. 73 ff.
164 Sorel (2003), p. 376; Kaetzler (2008), p. 174; BMF (2004), p. 86.
165 Hülsse (2008), p. 459 f.

> to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse."[166]

The FATF was founded in 1989 during the G7 summit in Paris, and is now accommodated on the premises of the OECD headquarters in Paris. It counts 36 members, among which are the EU-15 Member States, Norway, Iceland, Switzerland, Turkey, and the European Commission as an individual member.[167]

The FATF is one of the most important driving forces in the development of international anti-money laundering legislation. In 1990, the FATF has first published its 40 Recommendations, outlining the measures that should be taken by all countries in order to identify the potential risks and find ways to adequately respond to these risks. The Recommendations were originally intended to combat the laundering of revenue generated by the sale of illegal substances.[168] However, they were soon (in 1996, to be exact) updated to include the laundering of other types of criminal proceeds as well.[169] From 2001 on, nine Special Recommendations were added, which specifically addressed the risk of terrorist financing.[170] The most recent revision in 2012 updated the Recommendations, and integrated the Special Recommendations into the scope of the forty Recommendations.[171] The FATF's Recommendations are the basis for the latest updates of the European anti-money laundering framework.[172]

166 FATF Recommendations (2012), p. 7. See also BMF (2004), p. 86; Razavy/Haggerty (2009), p. 142.

167 These Members are mentioned explicitly because these Members therefore (1) together make up the majority of Members of the group which is the driving force behind the internationally coordinated fight against money laundering and terrorist financing and (2) are all bound to the ECHR, which bids them respect the right to privacy. As this thesis is dedicated to the compatibility of the former with the latter, the involvement of these European states with both the FATF and the ECHR is significant. This connection will also be further discussed in Chapter IX section i below.

168 FATF Recommendations (2012), p. 7; Sorel (2003), p. 373.

169 FATF Recommendations (2012), p. 7.

170 FATF Recommendations (2012), p. 7.

171 FATF Recommendations (2012), p. 7.

172 COM (2016) 450, p. 4; Kaetzler (2008), p. 174.

The FATF also regularly publishes special reports on topics, in which a risk of money laundering or terrorist financing was identified. In this way, the FATF has published a report on Hawala in October 2013 and one on virtual currencies in June 2014.[173] Besides these reports, the FATF also examines national rules and the application of the FATF standards periodically very closely, and evaluates whether the national implementation of the FATF's own Recommendations are satisfactory. The reason for such evaluations is that it has been recognised that in the increasingly globalised financial sector, it has become very simple for both money launderers and terrorist financiers to shift their operations to a state with less stringent regulation, from which the financial sector of all other countries is quickly accessible.[174]

It is important to note that the FATF's evaluations are not limited to its own member jurisdictions.[175] Instead, the FATF also on its own initiative evaluates the legal situation of third countries to determine whether legislation correctly reflects the FATF standards.[176] The outcome of these evaluations can have an immediate impact on an evaluated jurisdiction. In the event of a negative judgment, the FATF can blacklist a jurisdiction. As of April 2017, only North Korea and Iran are fully blacklisted,[177] but nine other jurisdictions are on the list of "other monitored jurisdictions",[178] among which is Bosnia and Herzegovina.[179] It should be noted, however, that the FATF has been criticised strongly for not going far enough in its assessment of high-risk countries. The European Economic and Social Committee, for instance, has found clear words to criticise the fact that the FATF does not include the most notorious tax havens in its list of high-risk jurisdictions:[180] "It is regrettable that a body such as the FATF, which carries out such important work

173 See FATF Hawala (2013) and FATF virtual currencies (2014).
174 Sorel (2003), p. 378.
175 Hülsse (2008), p. 464.
176 Sorel (2003), p. 374.
177 See http://www.fatf-gafi.org/countries/#high-risk (last accessed 3 January, 2018). See also Hülsse (2008), p. 461 f.
178 See http://www.fatf-gafi.org/countries/#high-risk (last accessed 3 January, 2018).
179 This is significant as Bosnia and Herzegovina has submitted its application to join the European Union on the 15th of February 2016.
180 In particular, the tax havens used according to the 'Panama Papers' as well as recently the 'Paradise Papers' are missing from the list of high-risk countries, despite the Panama Papers being one of the main reasons given for the proposal of the fifth Anti-money laundering Directive. Note however that 6 of the 21 territories named in the Panama Papers are EU Member States or territories dependent on an EU Member State. See European Economic and Social Committee 13666/16, p. 6, 8. See also Schmidt/Ruckes (2017), p. 473 ff.; Beckschäfer (2017), p. 41 f.

in analysing international financial crime and in proposing means to combat it, has not found an appropriate way of drawing up its lists of high-risk countries."[181]

However, when a jurisdiction is once listed on the FATF blacklist, the consequences can reach far, as the FATF urges "its members and other jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from the jurisdiction".[182] This enhanced due diligence can have the effect of blocking financial institutions from countries on the blacklist to be effectively barred from the international financial market, and are therefore considered to be very effective.[183]

Critique expressed by the FATF in its evaluations of national anti-money laundering systems is taken very seriously by most governments and lawmakers.[184] For instance in Germany, the provision on money laundering in the criminal code (*Strafgesetzbuch,* StGB)[185] had to be changed, because the provision explicitly excluded perpetrators of the predicate offence from being additionally punishable for money laundering.[186] Punishing an individual for both a predicate offence and the subsequent money laundering is seen by many commentators as being in conflict with the principle *ne bis in idem*.[187] The FATF demanded that this gap be closed, with which the lawmaker promptly complied by adding a third sentence to the same paragraph of article 261 StGB, in which the exclusion of punishment of the perpetrator of the predicate offence is inapplicable in the case where the perpetrator places an illegally obtained object into circulation, concealing the origin of that object. This addition has been received very critically by the majority

181 European Economic and Social Committee 13666/16, p. 9. See also Fläming (2007), p. 2.
182 See the latest FATF public statement from February 24th, 2017 http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-february-2017.html (last accessed 3 January, 2018).
183 Countries other than Iran and North Korea have generally not stayed on the FATF's lists for more than two consecutive years, as they scrambled to update their systems and to achieve a level sufficient to be delisted. See for example the FATF statement of June 2013, in which it delisted five jurisdictions and was working with 21 other jurisdictions on improving their systems, http://www.fatf-gafi.org/publications/fatfgeneral/documents/compliance-june-2013.html (last accessed 3 January, 2018).
184 See, however, Lennon/Walker (2009), p. 41.
185 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 11.06.2017 (BGBl. I S. 1612) m.W.v. 01.07.2017.
186 Article 261 (9), second sentence of the German criminal code (StGB). See also Walter (2009), p. 571 f. for the situation in the United Kingdom.
187 Weigell/Görlich (2016), p. 2183. See also Arzt (1990), p. 5.

of German commentators in criminal law,[188] and it is not at all certain that this revised provision would be upheld if it were challenged before the Constitutional Court.[189]

### iii. Developments in Europe

Meanwhile, developments in Europe closely followed the legal innovations in the United States. The first important anti-money laundering document on the European level was Recommendation (80)10,[190] adopted by the Council of Europe in 1980. This Recommendation essentially demands that customers must be identified when they open an account or deposit, and when they carry out a transaction of a certain magnitude. In addition, banks were to be enabled to identify bank notes involved in criminal offences.[191]

With this Recommendation, the development of European anti-money laundering legislation began. It was soon taken up by the European Union. The first Anti-Money Laundering Directive 91/308/EEC (1AMLD)[192] was designed along similar lines. It was passed in 1991 on the European Union level. This Directive contained a first outline of the European anti-money laundering framework, and was largely based on the 1990 FATF standards. Importantly, the Directive contained a positive obligation on Member States to make money laundering a criminal offence, but does not yet mention or apply to terrorist financing.

The first Anti-money laundering Directive applied to credit institutions and financial institutions (article 1 1AMLD), but not yet to any non-financial service provider, such as lawyers. The obligations conferred upon those obliged entities are already rather burdensome, but still rather limited compared to the current standards. The obligations were initially structured as follows: In the first place, customers had to be identified when a business relationship is commenced. If the

188 Weigell/Görlich (2016), p. 2183, with additional references.
189 See also the remarks made in Chapters IX and X below on the incompatibility of the Anti-money laundering Directive with the case law of the German Constitutional Court.
190 Recommendation No. R(80)10 of the Committee of Ministers to Member States on Measures against the Transfer and the Safekeeping of Funds of Criminal Origin. Adopted by the Committee of Ministers on 20 June 1980 at the 321st meeting of the Ministers' Deputies.
191 This reflects the response to the wave of kidnappings for ransom carried out in many different Member States throughout the 1960's and 1970's.
192 Council Directive 91/308/EEC of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering, OJ L 166, 28.6.1991, p. 77–82. See also Kätzler (2008), p. 174.

transaction was not linked to a business relationship, but rather an occasional transaction, or a series of such occasional transactions appearing to be linked, the customer had to be identified when a transaction amounting to 15,000 European Currency Units (ECU) was carried out. The customer due diligence duties were not yet as complex, but simply amounted to a duty to "examine with special attention any transaction which they regard as particularly likely, by its nature, to be related to money laundering" (article 5 1AMLD). When such an examination raised any red flags, the obliged entity must proactively inform the competent authorities.[193] FIUs would only be established under a Council Decision in 2000, after the international cooperation among the different competent authorities proved difficult.[194] Finally, the first Anti-money laundering Directive already contained a prohibition of tipping off, a duty to retain identification and transaction data for five years, and an obligation on Member States to apply appropriate sanctions for non-compliance with the anti-money laundering obligations.

In 1996, the FATF updated its Recommendations to address technological developments which could be exploited for the purpose of money laundering, and to close identified lacunae in the existing framework. The European anti-money laundering framework was accordingly updated to reflect the FATF's newest standards with the second Anti-money laundering Directive.[195] The negotiations about this Directive were very difficult, and took over two years, and may have taken even longer if the post-9/11 effort of the United States to increase anti-money laundering standards worldwide had not also reached and influenced Europe.[196] One of the main conflicts making the negotiations so difficult was the European Commission's intended extension of the circle of obliged entities beyond the limits demanded by the FATF. In particular lawyers and notaries were now to be included in the list of obliged entities.[197] The European Parliament had

193 See Mitsilegas/Gilmore (2007) p. 122 for more information on the three different models of competent authorities the Member States were developing in the absence of a uniform FIU network. See also Hetzer (2002), p. 412.

194 Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000.

195 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 - Commission Declaration, OJ L 344, 28.12.2001, p. 76–82.

196 Mitsilegas/Gilmore (2007) p. 123.

197 Sorel (2003), p. 376; Hetzer (2002), p. 408. See also CJEU Case C-305/05, *Ordre des barreaux francophones et germanophone and Others v Conseil des ministers* [2007]. See also Tracfin annual report 2015, p. 23.

misgivings "regarding the impact of the extension of the Directive's duties to the legal profession in terms of the right to a fair trial and the principle of lawyer-client confidentiality."[198] Besides lawyers and notaries, the personal scope of the second Anti-money laundering Directive was also extended to auditors, real estate agents, casinos, and dealers in high-value goods when they accept a cash payment of EUR 15 000 or more. In addition, the identification duties were to be observed by each of those obliged entities and intensified compared the first Directive. Finally, the second Directive refers to a number of specified predicate offences, and to the concept of 'serious crime'.

It should be noted in this context that another reason for the slow movement of the negotiations of this Directive was that the financial sector did not back it. *Bures* refers to a 2004/05 survey of British financial services providers, in which "almost two-thirds of the respondents said the existing AML measures were too severe in proportion to the risks of money laundering."[199] One may say that the financial sector considered the anti-money laundering measures to be disproportionate.[200]

**iv. The Patriot Act**

It was mentioned earlier that the Know Your Customer rules were not, on the whole, met with enthusiasm upon their first proposal in the United States. This, however, changed in 2001. Only a couple of years after the Know Your Customer rules were rejected due to civil liberties concerns, the political climate suddenly underwent so radical a change that those rules could pass through the United States legislature in record time.[201] The attacks of September 11th, 2001 triggered a radical response by the government,[202] passing the USA Patriot Act[203] only six weeks later, in an unprecedented legislative effort.

198 Mitsilegas/Gilmore (2007) p. 123.
199 Bures (2015), p. 229.
200 See for a detailed discussion of the proportionality of the anti-money laundering measures in their current form Chapter IX below.
201 Ryder (2007), p. 822; Razavy/Haggerty (2009), p. 143. See in this context also Korff (2014), p. 92; Golden et al. (2011), p. 515.
202 See in this context also Mezzana/Krlic (2013), p. 5; Razavy/Haggerty (2009), p. 142 f.; Shields (2005), p. 28.
203 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Pub. L. No. 107-56, 115 Stat. 272 (2001), codified as amended in different sections of 12, 15, 18, and 31 U.S.C.), commonly referred to as (USA) Patriot Act.

> "The Patriot Act was enacted with remarkably little deliberation. The huge anti-terrorism package, covering 350 different subject areas and forty different agencies, was pushed through Congress in less than a month. The law was hammered out in private negotiations between the Justice Department and party leaders; there were no final hearings to allow dissenters a voice in the process, no committee reports, no conference committee, and indeed, most members of Congress did not even have the opportunity to read the legislation."[204]

The political climate of the time allowed for such an irregular law-making procedure,[205] and it allowed for anti-money laundering rules previously deemed unacceptable due to human rights concerns to pass into law.

The Patriot Act brought about the codification of the Know Your Customer rules. In particular, customers of the banking sector need to be identified, and the identity verified as well as checked against blacklists of terrorist suspects.[206] The records of the identification procedure also needed to be retained by the institution. While before the rules of the Patriot Act entered into force, only some transactions triggered the duty to identify the customer, the Patriot Act now required customers to be identified at the beginning of the business relationship, independent of any further action.[207] Furthermore, some additional measures could be triggered if the Secretary of the Treasury identified an increased risk of money laundering, among others the duty to

> "(1) maintain additional records or make additional reports in connection with specific transactions; (2) identify the foreign beneficial owners of certain accounts; (3) identify the customers of a foreign bank who use interbank 'payable-through' accounts; (4) identify the customers of foreign banks who use interbank correspondent accounts; and (5) restrict or prohibit the opening or maintaining of certain interbank 'payable-through' or correspondent accounts."[208]

204 Gouvin (2003), p. 961. See also Lennon/Walker (2009), p. 39 for the similar occurrences in the United Kingdom.
205 See also Al-Jumaili (2008), p. 194.
206 Ryder (2007), p. 830 f.; Silvestri (2005), p. 167. See also CJEU Case T-47/03, *Jose Maria Sison v Council of the European Union* [2007]; and CJEU Case T-341/07, *Jose Maria Sison v Council of the European Union* [2011]. See also De Goede (2011), p. 506 f.
207 Gouvin (2003), p. 971. See also Korff (2014), p. 48 f.
208 Gouvin (2003), p. 971 f. See also Ryder (2007), p. 835 f.

Finally, the Patriot Act compelled compliance with these measures by imposing sanctions, including high fines.

There are a number of points which could be criticised about the USA Patriot Act. The irregular law-making procedure as well as the fact that the measures contained in the law have previously been considered to be in conflict with human rights have already been named earlier. Furthermore, it should be pointed out that the measures of the Patriot Act have increased the reporting duties falling on an increased number of obliged entities, exacerbating the previously already immense amount of paperwork with the authorities.[209] It should also be pointed out that while passed ostensibly in a package to design a framework for the protection and fight against terrorism,[210] it is not at all clear how the strengthened anti-money laundering rules are going to be useful for the fight against terrorist financing.[211] In fact, it is not clear whether the measures against the financing of terrorism have a significant impact on terrorism itself at all.[212]

**v. International Efforts to Combat Terrorist Financing**

Despite these severe points of critique of the measures contained in the Patriot Act, the standards set therein rapidly became the global standard for anti-money laundering legislation.[213] Before the events of September 11th, 2001, disrupting the financial support to terrorist organisations had already been identified as a potentially effective strategy to be pursued in the fight against terror.[214] However, at that time, terrorism was not yet necessarily recognised as a global phenomenon, but rather regarded to be a number of groups with certain (often political) aims, such as the RAF in Germany, the IRA in Northern Ireland, and the ETA in Spain. Governments dealing with such a terrorist group in their own territory could not always count on the support of their allies in combating the flow of financial support to those groups,[215] as many of the terrorist groups active at the time were following a specific political agenda, the combat of which was considered to be a

209 Gouvin (2003), p. 973; Hingst/Lösing (2012), p. 337.
210 See in this context also Ronellenfitsch (2007), p. 563.
211 Lennon/Walker (2009), p. 39. *Lennon* and *Walker* say that these provisions "were ghosted aboard".
212 See Gouvin (2003), p. 973 ff.; Ryder (2007), p. 829 f. See also the analysis of the impact of these measures on money laundering in Chapters IV (b) and IX of this book.
213 See also De Goede (2008a), p. 173 f.; Winer/Roule (2002), p. 88.
214 Ryder (2007), p. 822.
215 King/Walker (2015), p. 375; Lavalle (2000), p. 497.

domestic problem.[216] This is also reflected by, for instance, the support of the UN Convention on the Suppression of Terrorist Finance of 1999,[217] which had been signed by only four states, all of which were combating terrorism domestically before 9/11, and by 132 states worldwide by the end of 2003.[218]

The need for a rapid adoption of measures against the financing of terrorism and the fact that the system of anti-money laundering rules was already in place made the combination of the two a seemingly logical step. However, terrorist financing operations are fundamentally different from money laundering schemes.[219] As has already been explained above, while money laundering often involves complex multinational structures of shell companies and a number of different financial institutions, the financing of terrorism can potentially be exceedingly simple. Terrorist financing often only involves bringing funds into the possession of a terrorist group, and a transfer of funds is easily accomplished without suspicions raised anywhere.[220] Naturally, not all members of any terrorist group are known, and in a pinch other associates can carry out the transaction and/or carry physical cash to the group, thereby hiding the movement of the funds. However, terrorist financing can also be closely related to money laundering in that the funds to be transmitted to a terrorist organisation may be derived from criminal activity.[221]

This connection between the two concepts of terrorist financing and money laundering also made the FATF a logical organisation to turn to for support when the fight against the financing of terrorism was placed on the international agenda. The FATF received a mandate to extend its focus beyond money laundering to include terrorist financing in 2001, and reacted promptly by developing and adding nine Special Recommendations on countering the financing of terrorism to its 40 Recommendations on anti-money laundering.[222] Those Special Recommendations focus on a more effective strategy against terrorist financing. With the 2012 update, the Special Recommendations have been incorporated

216 As many terrorist groups were active predominantly in a limited geographic area, as the ETA in Spain and the IRA in Northern Ireland.
217 International Convention for the Suppression of the Financing of Terrorism, Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999, UN Treaty Series 2178, 197.
218 King/Walker (2015), p. 375. See also Ryder (2007), p. 830.
219 Sotiriadis/Heimerdinger (2009), p. 235; Zentes/Wybitul (2011), p. 92.
220 See also Lavalle (2000), p. 503.
221 King/Walker (2015), p. 382; Ryder (2007), p. 823.
222 FATF Recommendations (2012), p. 7 f.

into the 40 Recommendations as they apply to both money laundering and terrorist financing. Recommendations 5, 6, and 8 are the core Recommendations applicable to terrorist financing and the financing of proliferation, which is also to be counteracted with the same strategies.

FATF Recommendation 5 concerns guidance for the design of an effective criminal law approach against terrorist financing.[223] FATF Recommendation 6 concerns financial sanctions, such as the freezing of funds and assets,[224] blacklisting persons and entities,[225] and complying with the United Nations Security Council resolutions concerning terrorist financing.[226] This is of moment, as the freezing of assets is still one of the main tools used in the fight against terrorist financing,[227] the importance of which is emphasised by governments and courts on the national and European level.[228] However, the effectiveness of the freezing of assets is disputed, as it is seen to be "a short-term solution to a long-term problem."[229] The many different options available to terrorist organisations in generating and collecting funds renders the mere freezing of assets ineffective.[230]

FATF Recommendation 8 finally concerns Non-profit organisations, which have been proven to be vulnerable to abuse for terrorist financing operations, either by being established as a cover, or where an existing bona fide non-profit organisation's network is abused for terrorist financing operations.[231] The United States' strategy to combat terrorist financing concentrated particularly on non-profit organisations, suspected of funnelling funds from the United States to terrorist organisations abroad. However, although the funds of a number of charities were frozen in the aftermath of 9/11, the majority of these cases led to nothing. "In a vast majority of these cases the charges of supporting terrorism were either dropped or the US Government was unable to prove any connection with terrorist activities."[232]

223 FATF Recommendations (2012), p. 37 f.
224 Bures (2015), p. 216.
225 De Goede (2011), p. 506 f.; Winer/Roule (2002), p. 88 f.; Bures (2015), p. 218.
226 FATF Recommendations (2012), p. 39 ff. Recommendation 7 in essence repeats the same approach but targeting proliferation rather than terrorist financing. See also Sorel (2003), p. 374 f.; Ryder (2007), p. 830 f.
227 Ryder (2007), p. 832; Lavalle (2000), p. 492; Al-Jumaili (2008), p. 199.
228 Bülow (2013), p. 615; Al-Jumaili (2008), p. 199.
229 Ryder (2007), p. 835.
230 Ryder (2007), p. 835.
231 FATF Recommendations (2012), p. 54 ff. See also Raphaeli (2003), p. 62 f.
232 Ryder (2007), p. 834 f.

**vi. Recent Developments in Europe**

To return to tracing the development in Europe, the second and third Anti-money laundering Directives were helped along very much by the stipulations of the Patriot Act. The second Anti-money laundering Directive had been passed in December 2001 on the wave of efforts against money laundering and terrorist financing spearheaded by the United States.[233] Negotiations for this Directive had, however, been begun in 1999, and the text had not yet been updated to reflect the rapid developments taking place internationally in that area since September 11th, 2001. The Commission therefore brought a new proposal for a third Directive forward in 2004, again updating and strengthening the then still relatively new rules. The proposal for the third Directive[234] was triggered by the FATF Recommendations, which were revised in 2003 to reflect the newest developments in money laundering, and to which were added the Special Recommendations concerning terrorist financing. Surprisingly, the negotiations for this third Anti-money laundering Directive went very smooth compared to that of the second,[235] although the framework was again tightened, and the text tripled in size.[236]

The biggest change introduced in the third Anti-money laundering Directive is then of course the addition of terrorist financing to money laundering as the two crimes which are to be countered with the measures of the Directive. But the framework was also updated in other areas, particularly concerning customer due diligence. The third Directive embraces a risk-sensitive approach, with applicable simplified and enhanced customer due diligence measures depending on the risk each transaction may pose.[237] Anonymous accounts and passbooks were expressly prohibited. Furthermore, the provisions concerning reporting duties have undergone a significant change compared to the second Anti-money laundering Directive, with the express inclusion of Financial Intelligence Units into the text, and a section charting the duties and competences of the FIUs. In those provisions, FIUs are given broad powers with few limits, in particular no limitations due to

233 Ryder (2007), p. 838. See also Mezzana/Krlic (2013), p. 5; Ronellenfitsch (2007), p. 564; Warde (2007), p. 236.

234 Directive 2005/60/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 (Text with EEA relevance), OJ L 309, 25.11.2005, p. 15–36.

235 Mitsilegas/Gilmore (2007) p. 125.

236 The text of the Directive went from 6 to 22 pages, the number of articles increasing from 18 to 47, with increasingly difficult subject matter besides.

237 Glos/Hildner/Glasow (2017), p. 86 f.

data protection and privacy safeguards. Protection of legal professionals and former exemptions have been dissipated to a large extent.[238]

In addition to the European Union, the Council of Europe also became active in the field of anti-money laundering and combating terrorist financing. The measures contained in the Patriot Act, demanded by the FATF and codified in the Directive also had an impact on the rest of the European continent, outside of the limits of the European Union. In 2005, Convention 198 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (C198)[239] was passed under the auspices of the Council of Europe. The Convention is now signed by 40 countries and organisations, including the European Union, and ratified by 29 countries, of which 11 countries are not European Union Member States.[240] Convention 198 is of immense practical importance as an international instrument.[241] However, the legal provisions outlined in the Convention have since been eclipsed on a EU level, as the measures contained in this instrument fall short in scope and detail of the demands of the FATF and indeed the fourth and proposed fifth Anti-Money Laundering Directives.[242]

The Convention does, however, serve as an extension of the anti-money laundering framework out of the limits of the European Union toward a pan-European approach, bringing the 11 non-European Member States ratifying the Convention into closer cooperation with their partners in the European Union. While it is not necessary to repeat here the content of the measures of the Convention, one striking thing should be pointed out, which is the fact that C198 fails to refer to the ECHR. The Convention does demand that when information is shared among Financial Intelligence Units, the recipient FIU must not further divulge received information (article 46 (10) of C198), and that shared information shall be protected by the standard applied to the requesting FIU under national law (article 46 (11) of C198). However, the Convention fails to demand that all

238 See a more detailed discussion in Mitsilegas/Gilmore (2007) p. 127 f.
239 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 16 May 2005, CETS No.198, Entered into Force on 1 May 2008.
240 At the time of writing, the United Kingdom is still counted as Member State of the European Union.
241 COM (2016) 50 final, p. 13.
242 See however COM (2016) 50 final, p. 9, mentioning the oversight of introducing a uniform criminal offence of terrorist financing on the European Union level.

processing of data pursuant of the anti-money laundering measures contained in the Convention must be in conformity with the demands of Article 8 of the ECHR and C108.[243]



## e. The Fourth Anti-Money Laundering Directive 2015/849

At this point in time, the European anti-money laundering framework is governed by the fourth Anti-money laundering Directive (EU) 2015/849, with a fifth Anti-money laundering Directive expected shortly. The fourth Anti-money laundering Directive has entered into force in June 2017, and is therefore one of the newest and most modern piece of anti-money laundering legislation currently in existence. It reflects the newest international standards, and its territorial scope covers the large European financial centres in London,[244] Paris, and Frankfurt.

### i. Obliged Entities

The anti-money laundering approach is largely based on sourcing duties out to private sector service providers.[245] The actors are addressed by the Directive are manifold. Essentially, the Directive addresses all actors either transferring value as a part of the nature of their business, or handling large amounts of cash or valuable items in commerce, employing several catch-all phrases throughout article 2 4AMLD.

In the first place, the principal addressees are credit institutions (article 2 (1) 4AMLD). Credit institutions are defined in article 3 (1) 4AMLD:

> "'credit institution' means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013[246] of the European Parliament and of the Council, including branches thereof, as defined in point (17)

243 See also Korff (2014), p. 94.
244 The United Kingdom is, at the time of writing, still a European Union Member State and therefore obliged to comply with its duty to implement European secondary legislation.
245 See for information on data exchange between public and private entities fundamentally Haase/Peters (2017), p. 2 ff.
246 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 Text with EEA relevance, OJ L 176, 27.6.2013, p. 1–337. Footnote added by the author.

> of Article 4(1) of that Regulation, located in the Union, whether its head office is situated within the Union or in a third country".

Regulation 575/2013, also called the Capital Requirements Regulation (CRR), defines credit institutions in article 4 (1) (1) CRR as "an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account". A branch of such an undertaking is "a place of business which forms a legally dependent part of an institution and which carries out directly all or some of the transactions inherent in the business of the institutions" (article 4 (1) (17) CRR). In essence, this means banks and their branch office. The term 'transaction' is not defined in the law, but can be considered to cover any action that purposes or causes a movement of property.[247]

Besides credit institutions, the second group of principal obliged entities are financial institutions (Article 2 (2) 4AMLD), which covers various entities, such as currency exchange offices, money transmitters, and remittance offices. The legal definition is included in article 3 (2) 4AMLD and reads as follows:

> "'financial institution' means:
>
> (a) An undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU[248] of the European Parliament and of the Council, including the activities of currency exchange offices (bureaux de change);
> (b) An insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC[249] of the European Parliament and of the Council, insofar as it carries out life assurance activities covered by that Directive;

247 Hetzer (2008), p. 562. See also Sotiriadis/Heimerdinger (2009), p. 234 with further references.
248 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 27.6.2013, p. 338–436. Footnote added by the author.
249 Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (Text with EEA relevance), OJ L 335, 17.12.2009, p. 1–155. Footnote added by the author.

(c) An investment firm as defined in point (1) of Article 4(1) of Directive 2004/39/EC[250] of the European Parliament and of the Council;
(d) A collective investment undertaking marketing its units or shares;
(e) An insurance intermediary as defined in point (5) of Article 2 of Directive 2002/92/EC[251] of the European Parliament and of the Council, where it acts with respect to life insurance and other investment-related services, with the exception of a tied insurance intermediary as defined in point (7) of that Article;
(f) Branches, when located in the Union, of financial institutions as referred to in points (a) to (e), whether their head office is situated in a Member State or in a third country"

The most important points of this definition and simultaneously the points that might need further clarification are the above-mentioned "activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU". Directive 2013/36/EU is the Capital Requirements Directive (CRD), in the Annex of which are listed the activities of financial institutions. Those activities include, inter alia, lending, financial leasing, the provision of payment services, guarantees and commitments, foreign exchange, money broking, and portfolio management. In essence, therefore, financial institutions are all financial services providers other than credit institutions.

Furthermore, a number of legal or natural persons, who in their line of business handle large sums of money or deal in valuable property, are obligated to comply with the measures set forth in this Directive.[252] The natural and legal persons addressed are, among others, auditors, accountants and tax advisors, but also notaries,[253] real estate agents and gambling services (Article 2 (1) (a)-(f) 4AMLD). Those professionals are considered to "have a quite wide range of means to launder money", and are therefore "much sought-after covers."[254] In detail, the Directive covers:

250 Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC, OJ L 145, 30.4.2004, p. 1–44. Footnote added by the author.
251 Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation, OJ L 9, 15.1.2003, p. 3–10. Footnote added by the author.
252 Sandleben/Wittmann (2010), p. 265.
253 Notaries are the most important group of obliged entities outside of the conventional financial sector. See Tracfin annual report 2015, p. 23.
254 Sorel (2003), p. 376.

"the following natural or legal persons acting in the exercise of their professional activities:

(a) Auditors, external accountants and tax advisors;
(b) Notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:
    (i) Buying or selling of real property or business entities;
    (ii) Managing of client money, securities or other assets;
    (iii) Opening or management of bank, savings or securities accounts;
    (iv) Organisation of contributions necessary for the creation, operation or management of companies;
    (v) Creation, operation or management of trusts, companies, foundations, or similar structures;
(c) Trust or company service providers not already covered under point (a) or (b);
(d) Estate agents;
(e) Other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
(f) Providers of gambling services."

Therefore, in principle, all natural or legal persons professionally working with large amounts of money or valuable property are covered by the third group. Cash transactions are included not only because the origins of cash are very difficult to trace, but also because luxury goods are easily moved and re-sold at little loss, and can thus also be used as a vehicle for funds transfer.[255]

The list of obliged entities has been continually expanded with the different versions of the Anti-money laundering Directive.[256] In this way, the first Anti-money laundering Directive only applied to credit institutions and financial

255 See above within the same chapter for a definition of the terms 'property' and 'funds', and see Chapter III (c) below for a discussion of cash.
256 Sandleben/Wittmann (2010), p. 265.

institutions, although the recitals of the Directive point out that "Member States must extend the provisions of this Directive in whole or in part, to include those professions and undertakings, whose activities are particularly likely to be used for money laundering purposes" (recital 18 1AMLD).

This was changed with the second Anti-money laundering Directive, which inserted an article 2a 2AMLD that formally extended the scope of the Directive to selected professions, such as tax advisors, real estate agents, and casinos (article 2a 2AMLD). The same article furthermore also included "dealers in high-value goods, such as precious stones or metals, or works of art, auctioneers, whenever payment is made in cash, and in an amount of EUR 15 000 or more" (article 2a (6) 2AMLD).

The third Anti-money laundering Directive closed loopholes in this definition. In this way, the Directive covered besides credit institutions and financial institutions also auditors, tax advisors, and legal professionals (article 2 (1) (3) (a) and (b) 3AMLD) as the previous Directive did, but adding "trust or company service providers not already covered under points (a) or (b)" to ensure that no obliged entity could escape its obligations through its administrative organisation. In addition, the provision covering dealers in high-value goods was changed slightly, now reading "other national or legal persons trading in goods, only to the extent that payments are made in cash and in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked" (article 2 (1) (3) (e) 3AMLD).

The fourth Anti-money laundering Directive again sharpened the focus, and closed off potential loopholes in the enumeration of obliged entities, now covering estate agents rather than real estate agents, in order to ensure that letting agents are also included (recital 8 4AMLD). In addition, the definition of obliged traders in goods was slightly sharpened compared to the previous Directive, and the reporting threshold was notably lowered from EUR 15 000 to EUR 10 000.[257] In addition, the Directive now applies to "providers of gambling services" rather than to casinos, closing off a potential loophole if casinos are only defined as gambling services providers with their own brick-and-mortar premises (recital 21 4AMLD).

257 The original proposal of the fourth Anti-money laundering Directive intended to lower the threshold to EUR 7 500, see COM (2013) 45, p. 9.

Looking ahead into future amendments to the framework, the upcoming fifth Anti-money laundering Directive will again extend the personal scope of the Directive, in that providers of services connecting to the virtual currency environment are to be included. The entities that are to be covered are firstly services exchanging virtual currencies for fiat currencies, and secondly so-called custodial wallet providers, which are essentially services keeping virtual currency units safe for their customers. Virtual currencies are introduced in great detail in the following Chapter III, and the extension of the scope of the Anti-money laundering Directive to virtual currency applications is discussed below in Chapter IV.

**ii. Financial Intelligence Units**

Before going into details concerning the obligations of obliged entities, a few words should be said about the authorities entrusted with specific anti-money laundering tasks, the Financial Intelligence Units. It has already been mentioned that FIUs were originally established under a Council Decision in 2000,[258] and since the third Anti-money laundering Directive, they and their work are an integral element of the anti-money laundering strategy employed on the European level.

The rules concerning FIUs and their work have continually been expanded, from only some general remarks made on the work of FIUS in article 21 3AMLD to a detailed description of the organisation and tasks of FIUs in article 32 4AMLD. The rules contained in the fourth Anti-money laundering Directive concerning FIUs are furthermore expected to be further clarified in the upcoming fifth Anti-money laundering Directive.[259]

In essence, FIUs are entities established in each Member State, which specialise in anti-money laundering and countering the financing of terrorism. Their task is to receive suspicious transactions reports from obliged entities and to lead the prevention and investigation into money laundering and terrorist financing schemes.[260] Recital 14a 5AMLD puts the purpose, tasks and obligations of the FIU as follows:

258 Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000. See also Hetzer (2002), p. 411.
259 COM (2016) 450, p. 13 f.
260 Hetzer (2002), p. 410.

> "The purpose of the FIU is to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing, and to disseminate the results of its analysis as well as additional information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorism financing. With respect to this analysis function, it is essential that FIUs can exchange with other FIUs any information that may be relevant for the processing or analysis of information related to money laundering, associated predicate offences and terrorist financing regardless of the type of associated predicate offence and even if the type of associated predicate offence is not identified at the time of the exchange. FIUs should not refuse the exchange of information to other FIU, spontaneously or upon request,[261] for reasons such as lack of identification of associated predicate offence, features of criminal national laws, differences of associated predicate offence definitions or reference to particular associated predicate offences. Similarly FIUs should grant their prior consent to forward the information to competent authorities regardless of the type of possible associated predicate offences in order to allow the dissemination function to be carried out effectively. In any cases differences between national law definitions of associated predicate offences should not limit the exchange, the dissemination to competent authorities and the use of this information as defined in this Directive. Such measure applies to all forms of associated predicate offences. Having regard to the fact that FIUs have reported difficulties in exchanging information based on differences in national definitions of some of the associated predicate offences which are not harmonised under the European law, such as tax crimes, such differences in national law should not hamper the exchange, dissemination and use of such information by and between FIUs."[262]

The FIU is therefore an independent agency with a particular emphasis on the collection and processing of information. In essence, it is the first point of contact

261 See in this context also Korff (2014), p. 101. Footnote added by the author.
262 Recital 14a of the fifth Presidency compromise text 15605/16.

for all issues relating to money laundering and terrorist financing.[263] The task of the FIU is to receive and analyse information forwarded by obliged entities, and to forward the results of their analysis to the national authorities competent to begin a formal criminal investigation (article 32 (3) 4AMLD). In addition to receiving information, the FIU can furthermore request information from obliged entities. While at this point in time some states have limited the FIU's options to demand information from obliged entities to requesting additional information from an entity which had previously forwarded a suspicious transaction report, the upcoming fifth Anti-money laundering Directive will extend this option. In the words of the Commission, "FIUs should be able to obtain additional information from obliged entities, and should have access on a timely basis to the financial, administrative and law enforcement information they require to undertake their functions properly even without there having been a suspicious transaction report."[264] It can therefore be said that the powers of the FIU are large and continually in the process of being further expanded.

### iii. Obligations

The obligations conferred on obliged parties are aimed at ensuring that the financial services offered by obliged parties are not abused for the purposes of money laundering or the financing of terrorism.[265] In the first place, obliged entities are bound to identify each customer, and to record and verify the customer's identity (article 11 in connection with article 13 4AMLD). Furthermore, according to article 13 (1) (d) 4AMLD, the service provider is to monitor all transactions carried out by each customer to make sure that nothing suspicious escapes his notice:

> "conducting ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that documents, data or information held are kept up-to-date".

263 Hetzer (2002), p. 411 f.
264 COM (2016) 450, p. 14.
265 See also Leslie (2014), p. 120 ff.

A business relationship is in this context defined as "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" (article3 (13) 4AMLD).[266] In addition, if suspicious activity is noticed, the entity is obliged to report this activity to the authorities in his Member State: "all suspicious transactions, including attempted transactions, shall be reported" (article 33 (1) 4AMLD). Finally, identification information and transaction records must be retained for at least five years after the end of a business relationship (article 40 (1) 4AMLD).

This means that the obligations obliged entities are charged with can be roughly divided into a four-tier structure of identification, monitoring, reporting, and retention. The first three concepts are also known as know your customer (KYC), customer due diligence (CDD) and suspicious transactions reporting (STR). The idea is that all financial transactions must have an identifiable person on the side of the sender of the funds as well as on the side of the recipient. The financial services provider carrying out the transaction is obliged to continually monitor all in- and outgoing transactions for suspicious activity of any description, to notify the national financial intelligence unit of any suspicious transactions that have been detected, and finally to keep records for a specified length of time in order to ensure their availability in case they are wanted. All those obligations are now to be analysed in detail.

***(1) Identification of Customers***

The first obligation falling on all obliged entities is the duty to fully identify each customer. One of the central tools employed by the Directive against illicit flows of money is to make sure that every participant in financial transactions is identified. The Directive thus also demands of Member States to prohibit anonymous accounts and passbooks (article 10 (1) 4AMLD). This provision reflects FATF Recommendation 9, which concerns banking secrecy laws. The Recommendation reads, "Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations."[267] While the Directive is silent on banking secrecy as such, the prohibition on anonymous accounts in

266 Hetzer (2008), p. 562. See also Sotiriadis/Heimerdinger (2009), p. 236.
267 FATF Recommendations (2012), p. 14. See also Silvestri (2005), p. 167; Heine (2017), p. 368 ff.

combination with the other duties falling to obliged entities are very much in the spirit of the Recommendation.[268]

Each entity obliged to carry out customer due diligence measures under the Directive is obliged to apply measures "identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source" (article 13 (1) (a) 4AMLD).[269] Each natural person is thus obliged to present an ID card or passport, or other official document of this order, when he or she requests certain services from an obliged entity. This provision thus generally creates an environment in which every transaction between customers can be attributed to a fully identified sender and traced to a fully identified recipient.

If one of the participants is a legal person, the natural persons behind this legal person must also be fully identified. Legal persons could be used rather easily to form a convoluted system of shell companies in order to disguise the natural persons ultimately behind the legal person on either side of a financial transaction. In order to combat such systems, the beneficial owner of a company must be identified. Article 13 (1) (b) of the fourth Anti-money laundering Directive commits all obliged entities to take measures

> "identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer".[270]

A beneficial owner is "any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted" (article 3 (6) 4AMLD). This means that whenever an obliged

268 See also Schmidt/Ruckes (2017), p. 474 f.
269 Glos/Hildner/Glasow (2017), p. 86.
270 Note that the rules on beneficial ownership have been tightened considerably in the fourth Anti-money laundering Directive compared to the previous framework. See also Sotiriadis/Heimerdinger (2009), p. 238.

entity accepts a legal person as a customer, the ownership of that legal person must be determined. If the legal person is owned by another legal person, the owners of the parent company must also be identified, until ultimately one or more natural persons can be identified as owners of the company in question.

The rules concerning beneficial ownership date back to the first Anti-money laundering Directive, although at the time the identification of the beneficial owner was only included in the recitals. As recital 11 1AMLD reads,

> "Whereas ensuring that credit and financial institutions require identification of their customers when entering into business relations or conducting transactions, exceeding certain thresholds, are necessary to avoid launderers' taking advantage of anonymity to carry out their criminal activities; whereas such provisions must also be extended, as far as possible, to any beneficial owners".

This concept has evolved over time, and recognising that opaque *Matryoshka* systems of shell companies are a major obstacle to successful investigation into money laundering schemes,[271] the identification of the beneficial owner has taken a priority in anti-money laundering.[272] The framework has therefore been strengthened several times, but the fourth Anti-money laundering Directive for the first time introduced detailed rules about beneficial ownership, with an entire chapter of the Directive dedicated to this complex (articles 30 and 31 4AMLD). The most important innovations in this regard are that obliged entities must now fully identify the beneficial owner of a legal person, and that beneficial ownership information is kept in a central register that is not only open to FIUs[273] and obliged entities, but also to "any person or organisation that can demonstrate a legitimate interest" (article 30 (5) (c) 4AMLD).[274] The fifth Anti-money laundering Directive is expected to further enhance the framework by harmonising the rules on those registers to some extent, and to ensure that these registers are interconnected on the European level.[275] The Commission hopes that this will result in enhanced

271 Cuéllar (2003), p. 317 f.
272 COM (2016) 450, p. 15 f.; Kaetzler (2008), p. 177; Sotiriadis/Heimerdinger (2009), p. 236; Golden et al. (2011), p. 523 f.
273 Krais (2017), p. 105.
274 See also Göres (2005), p. 254; Schaub (2017), p. 1443 f.; Krais (2017), p. 98 ff.; Fisch (2017), p. 408 ff.
275 COM (2016) 450, p. 18 f. See also Krais (2017), p. 106.

transparency and that the identification of beneficial owners will become more efficient for obliged entities.[276]

Identification is the first duty falling on obliged entities, right at the beginning of the business relationship between the customer and the obliged entity. A customer is generally identified when a business relationship is first entered into (article 11 (a) 4AMLD). This is the rule, in any case, for financial services providers whose services are designed to continue over a longer period of time. This provision is thus applicable to credit institutions when a customer opens a new bank account, or when an accountant or tax advisor accepts a new client. If the financial services to be provided are not of a long-term nature, customer due diligence measures must be applied before the transaction is carried out. There are several different provisions for the different transactions.

In the first place, whenever an occasional transaction of a value of EUR 15,000 or more is carried out by an obliged entity, whether or not this amount is transacted "in a single operation or in several operations which appear to be linked" (article 11 (b) (i) 4AMLD). This provision applies to the work of a number of obliged entities, such as real estate agents, notaries, and lawyers, whenever they carry out a large transaction, such as the sale of immovable property. When the transaction concerns a transfer of funds, the threshold is lowered to EUR 1 000 (article 11 (b) (ii) 4AMLD).

Secondly, if the obliged party does not provide financial services at all, but is trading in goods, the customer must be identified according to the rules laid out in the Directive, when the transaction is valued at EUR 10,000 or more, even if this threshold is not reached in one transaction but rather in several, apparently linked transactions (article 11 (c) 4AMLD). This provision aims mainly at sellers of luxury articles.

In the third place, gambling services providers must identify a customer if an amount of EUR 2,000 is exceeded in "the collection of winnings, the wagering of a stage, or both" (article 11 (d) 4AMLD). Again, the threshold also applies to the cumulative value of linked transactions.

276 COM (2016) 450, p. 19. See critique by Krais (2017), p. 106 f.; Friese/Brehm (2017), p. 273.

Finally, beyond those transaction-based instances in which the obliged entity must carry out customer due diligence measures, the Directive mentions two further situations in which the customer must be identified. Those are article 11 (e) 4AMLD, "when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold", and article 11 (f) 4AMLD, "when there are doubts about the veracity or adequacy of previously obtained customer identification data." Therefore, the thresholds mentioned above are not rigid. Instead, transactions falling in value under the thresholds may still fall into the scope of the Directive if there is any suspicion that the obliged entity can identify. It should also be pointed out in this context that in some cases, the information on the identity of the customer may have to be checked and updated if necessary.[277] This will especially be the case where the ownership of legal persons is subject to change, which has an effect on the beneficial owner behind that legal person. The nature of the business relationship between the obliged entity and the customer may also be subject to change over time.[278]

It should be noted that an obliged entity cannot entertain a business relationship with a natural or legal person who has not been fully identified in accordance with these rules. When a natural or legal person cannot be identified, the obliged entity must not carry out any transactions on behalf of that person.[279] In the case that a business relationship already exists when doubts as to the accuracy of the identity of the customer arise, the obliged entity must halt the relationship until this deficiency could be remedied. If it cannot be remedied, the business relationship must be cancelled.[280] While this is naturally a rather severe incision into the obliged entity's freedom to conduct a business,[281] the importance of the fight against money laundering and terrorist financing is generally seen as of such importance as to warrant the interference with this right.[282]

In addition to the identification of the customer, other information about the customer may have to be collected by the obliged entity. In this way, the obliged entity is may collect information on the profession, assets and income of a

277 Sotiriadis/Heimerdinger (2009), p. 236.
278 Sotiriadis/Heimerdinger (2009), p. 236.
279 Sotiriadis/Heimerdinger (2009), p. 237.
280 Sotiriadis/Heimerdinger (2009), p. 237.
281 See also the seventh concern discussed in Chapter IX.
282 Sotiriadis/Heimerdinger (2009), p. 237.

customer.[283] This information is necessary for the assessment and filtering of unusual and suspicious transactions, as it establishes expectations as to the normal financial and payment behaviour of a customer.

A duty related to the identification of customers is that of checking customers against a number of lists of persons. In this case, the purpose of identification is not to ensure that in the case that financial crime is detected, there is a paper trail from one identified customer to another, but rather to ensure from the outset that persons with a higher risk are more strictly monitored,[284] or that a business relationship is not established in the first place.

In the first place, this concerns lists of terrorists and terrorist suspects as well as known associates. Those lists are compiled on an international level and made available to obliged entities.[285]

In the second place, this concerns politically exposed persons (PEPs). While in the previous third Anti-money laundering Directive, the group of PEPs was not clearly defined,[286] the fourth Anti-money laundering Directive creates a little more certainty. The list of PEPs includes among others heads of state and ministers, Members of Parliament or high-ranking party officials, members of high-level judicial bodies, diplomats, and the directors and board members of International Organisations (article 3 (9) 4AMLD). Politically exposed persons are considered to be vulnerable to corruption and therefore to money laundering.[287] While the

283 See Tracfin annual report 2015, p. 16.

284 Kaetzler (2008), p. 176; Bergles/Eul (2003), p. 275; Golden et al. (2011), p. 516 f.; Reimer/Wilhelm (2008), p. 240.

285 Note in this context that persons and entities placed on such lists are still facing severe difficulties when they find that they have been wrongfully listed. See CJEU Case C-402/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* [2008]; CJEU Case T-47/03, *Jose Maria Sison v Council of the European Union* [2007]. See also Ryder (2007), p. 832 f.; Arnauld (2013), p. 239 f.; Sotiriadis/Heimerdinger (2009), p. 239; Bergles/Eul (2003), p. 277; Al-Jumaili (2008), p. 192; De Goede (2008b), p. 303 f.

286 Kaetzler (2008), p. 176. Kaetzler found the academic discussion of the precise definition of the term PEP "absurd", as in practice, it was left up to the obliged entity whether it considered a particular customer as a risk or not, depending on the customer's own statements concerning their offices. This is still to some extent the case, though the clarified definition in article 3 (9) 4AMLD curtails the margin of appreciation of banks. In addition, while the discussion on the definition of PEP might not have much academic merit, it may still be considered important in the context of data protection and privacy as well as the right to non-discrimination.

287 Sorel (2003), p. 376; Kaetzler (2008), p. 176; Golden et al. (2011), p. 516 f.

previous third Directive targeted primarily foreign PEPs,[288] the fact that domestic office holders are not immune to corruption has been acknowledged in the fourth Anti-money laundering Directive. Therefore, business relationships with or transactions carried out for politically exposed persons are always considered to be of a higher risk, and enhanced customer due diligence measures are applied. Such measures consist of requiring senior management approval before establishing the business relationship (article 20 (b) (i) 4AMLD), establishing the source of property involved in transactions (article 20 (b) (ii) 4AMLD), and ensuring closer monitoring of the relationship (article 20 (b) (iii) 4AMLD).

In addition to the politically exposed persons themselves, family members, such as spouses, children, and parents of politically exposed persons (article 3 (10) 4AMLD) are to be subject to the same enhanced measures as PEPs themselves (article 23 4AMLD). The same applies furthermore to persons known to be close associates of a politically exposed person, such as persons known to have close business relationships with a politically exposed person (article 3 (11) 4AMLD). Those persons are also to be considered of higher risk and therefore subject to the enhanced customer due diligence measures of article 20 4AMLD.[289]

It almost goes without saying that the number of politically exposed persons is immense, and that the number of family members and close associates added to politically exposed persons creates a long list of persons which is difficult to compile and even more difficult to keep up to date, considering that persons holding political office are prone to be replaced periodically. It is simply impossible for obliged entities to keep their own accurate lists of PEPs, family members and associates. Instead, rather costly commercial lists are available, without any guarantees concerning the accuracy of these lists.[290]

***(2) Surveillance of Transactions***

Customer due diligence does not only mean that both ends of each transaction can be tied to a fully identified natural person. Each obliged entity is furthermore confronted with two further important obligations which go hand in hand: That of monitoring all transactions, and that of reporting suspicious activity.

288 Kaetzler (2008), p. 176.
289 See Bergles/Eul (2003), p. 279.
290 See Bergles/Eul (2003), p. 276 f.

These obligations again reflect the applicable FATF Recommendations.[291] Recommendations 20 and 21 concern suspicious transactions reports. Recommendation 20 very simply requires that each financial institution that forms the suspicion, or has reasonable grounds to form the suspicion that funds processed by it are derived from criminal operations or connected to terrorist financing must immediately inform the FIU of those suspicions.[292] This Recommendation is incorporated into and enlarged upon in articles 32-38 4AMLD, which contain elaborate details on the process of reporting. The same section contains the rules according to which national FIUs are to be set up in Member States. Recommendation 21 concerns non-disclosure of the fact that a suspicious transaction report has been made, and rules concerning indemnity. In the first place, the Recommendation demands that all "[f]inancial institutions, their directors, officers, and employees" are "prohibited by law from disclosing ('tipping-off') the fact that a suspicious transaction report" has been made.[293] The non-disclosure rules are incorporated in article 39 4AMLD. Recommendation 21 furthermore demands that the natural person acting on behalf of a financial institution by reporting suspicious activity must be

> "protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred".[294]

These rules are incorporated in article 37 4AMLD.

In the first place, an obliged entity must therefore strive to understand and assess "the purpose and intended nature of the business relationship" which it is going to enter into with the customer (article 13 (c) 4AMLD).[295] This assessment serves the evaluation of the risk profile of each customer, and it paves the way to assessing

291 Bures (2015), p. 211 f.
292 FATF Recommendations (2012), p. 19; Golden et al. (2011), p. 518. See also Amoore/de Goede (2008), p. 180.
293 FATF Recommendations (2012), p. 19; Kaetzler (2008), p. 179.
294 FATF Recommendations (2012), p. 19.
295 Sotiriadis/Heimerdinger (2009), p. 236; Zentes/Wybitul (2011), p. 94.

what sort of transactions will be considered a normal transaction as opposed to 'suspicious activity' for an individual customer.

The second obligation with which an obliged party must comply is found in article 13 (1) (d) 4AMLD, namely



> "conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date".

These obligations are mostly aimed at institutions which enter into a long-term business relationship with the customer, such as banks providing an account to the customer. In a first step, the obliged entity is thus held to carefully review the sort of transactions that it believes it may expect of the customer, based on the information collected on the customer's background. During the course of the business relationship, each transaction initiated and received by the customer must, on a second level, be run through a surveillance system. This system is to filter out and flag all transactions which do not accord with the pattern of transactions predicted to be followed by the customer, and which therefore, or for any other reason, raise a suspicion of money laundering.[296] The terms of the Directive therefore essentially send obliged entities out on a permanent fishing expedition in the accounts of their customers.[297]

In addition, the Directive speaks of suspicious transactions at various instances, but it fails to define what the term 'suspicious' precisely entails.[298] The parameters and settings applied to and by this surveillance program can be different from service provider to service provider, and are generally kept as a business secret.[299]

296 Kaetzler (2008), p. 178; Sotiriadis/Heimerdinger (2009), p. 236; Amoore/de Goede (2008), p. 180 f.
297 See also Maras (2012), p. 69.
298 Sotiriadis/Heimerdinger (2009), p. 234 f.; See also Gouvin (2003), p. 967 f. This intransparency is also the subject of the fourth concern to be discussed in Chapter IX.
299 See Kaetzler (2008), p. 175; Zentes/Wybitul (2011), p. 93.

*(3) Reporting of Suspicious Transactions*

When the automated monitoring system has flagged any activity as suspicious or unusual, this activity will be reviewed by a trained anti-money laundering officer.[300] This person will check the flagged transaction and filter out false positives.[301] Once a transaction was identified as suspicious, the information pertaining to this transaction must be forwarded to the national Financial Intelligence Unit.[302] Article 33 (1) 4AMLD reads,

> "Member States shall require obliged entities and, where applicable, their directors and employees, to cooperate fully by promptly:
>
> (a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and
> (b) providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.
>
> All suspicious transactions, including attempted transactions, shall be reported."

In principle, obliged entities are not permitted to carry out transactions if they suspect that the proceeds of crime are involved. Instead, such a transaction should be stopped and reported to the FIU, which will then issue further instructions to the obliged entity (article 35 (1) 4AMLD). If, however, following this procedure "is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected operation", the financial service provider must carry out the transaction and forward all information to the FIU immediately thereafter. How an obliged entity is to know when carrying out a transaction would be inconvenient to law enforcement authorities is not specified in the text of the Directive.

300 Zentes/Wybitul (2011), p. 92.
301 Zentes/Wybitul (2011), p. 92; Bergles/Eul (2003), p. 275.
302 See also CJEU Case C-212/11, *Jyske Bank Gibraltar Ltd v Administración del Estado* [2013].

Finally, obliged entities are prohibited from informing the customer or any third parties of the fact that information about a suspicious transaction has been forwarded to the FIU (article 39 (1) 4AMLD).[303]



Monitoring and reporting duties are therefore the backbone of the currently applicable customer due diligence approach against money laundering. However, the effectiveness of these duties has been seriously questioned on numerous grounds.[304] In the first place, these duties have first been introduced in the Patriot Act, as a direct response to the events of September 11th, 2001.[305] However, it is generally acknowledged that these rules, had they been in place at the time of the attack, could not have prevented it.[306] Apart from the example of this specific attack, it is also questionable whether the monitoring and reporting duties have a tangible effect on money laundering and terrorist financing in general. *Ryder* cites several early studies conducted soon after September 11th, 2001, which have also brought such concerns forward, and notes that the concerns voiced in those studies had not been alleviated by 2007.[307] In response, it has been argued that it would be better to use the resources tied up in compliance with the monitoring and reporting duties of financial institutions could be better used in developing and implementing a different strategy.[308] The Economist is quoted with the argument that particularly in the area of terrorist financing, the "practical use of data about transactions is after an attack, when there might be some chance of tracing links in the networks that sustain terrorist movements."[309]

***(4) Record Keeping***

Finally, all obliged entities are compelled to archive a large amount of data. As article 40 (1) 4AMLD specifies,

> "Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose

303 Müller/Starre (2014), p. 24; Hetzer (2008), p. 564; Dittrich/Trinkaus (1998), p. 345. See also Göres (2005), p. 255; Maidorn (2006), p. 3754.
304 See also Dittrich/Trinkaus (1998), p. 347. The following section (g) goes into more detail concerning critique of the anti-money laundering approach.
305 See in this context also Waldron (2003), p. 200.
306 Ryder (2007), p. 836 f.
307 Ryder (2007), p. 846. See also Mezzana/Krlic (2013), p. 5.
308 Ryder (2007), p. 846.
309 *The Economist* of 22nd October 2005, quoted in Ryder (2007), p. 847.

of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;
(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.

Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years."

In the first place, the obliged entity must therefore retain a record of the identification records used in the customer due diligence check originally carried out when the business relationship was first begun (article 40 (1) (a) 4AMLD). This concerns the information collected on the identity of all customers, including of beneficial owners. In the second place, obliged entities are compelled to retain a record of transactions (article 40 (1) (b) 4AMLD). This second category of data concerns the data collected about transactions between identified customers. Both categories of data must be retained for a period of five years after the end of the business relationship, or, when there was no long-term business relationship, after the transaction. In addition, Member States can exceptionally extend the retention period to a maximum of ten years.

It must be pointed out that the retention obligation is not limited to cases in which suspicion has been formed, or even to cases of higher risk. Instead, the obligation to retain data is applicable to all customers of an obliged entity. It must be pointed out in this context that this retention obligation therefore leads to a large amount of stored data, which is of no practical use to law enforcement,[310] but which instead poses a liability to the obliged entity and a security risk to the data subject.[311]

These data retention obligations reflect FATF Recommendation 11, which, however, limits its scope largely to fixing a minimum retention period to five years and to demanding that the retained "transaction records should be available to domestic competent authorities upon appropriate authority."[312] The five year retention period has been operated in similar terms since the first Anti-money laundering Directive.[313] In this way, article 4 1AMLD required the retention of identification documents for "at least" five years after the end of the business relationship, a rule which has been largely left unaltered over the course of the four Directives, except that the words "at least" are eliminated from the text of article 40 (1) (a) 4AMLD. Similarly, the first Anti-money laundering Directive required the retention of transaction records for a period of, again, "at least" five years after the transaction was executed. This latter rule has been changed in Article 30 (b) 3AMLD to read "for a period of at least five years following the carrying-out of the transactions or the end of the business relationship." The precise length of the retention period therefore depended on the implementation into national law. The fourth Anti-money laundering Directive again changed the rules slightly, to set the retention period of both the transaction records and identifying information to five years after the end of the business relationship (article 40 (1) (a) and (b) 4AMLD).

Article 40 (1) 4AMLD goes on to order obliged entities to remove all personal data after this period. However, there is the broad exception already mentioned, which grants Member States the power to extend the retention period for another five years, if the Member State deems such a longer retention period necessary and

310 Dittrich/Trinkaus (1998), p. 347. *Dittrich* and *Trinkaus* spoke of "data graveyards" generated by the retention obligation as early as 1998.
311 Mehrbrey/Schreibauer (2016), p. 78 f.; Karper (2006), p. 217. See also BaFin (2016), p. 67 f.; Cannataci (2013), p. 12.
312 FATF Recommendations (2012), p. 15; Golden et al (2011), p. 518 f.
313 Dittrich/Trinkaus (1998), p. 345.

proportionate (article 40 (1) 4AMLD). Article 40 4AMLD therefore allows for a retention period of a total of ten years after the end of the business relationship between the obliged entity and the customer, and therefore goes far beyond the expectations set by FATF Recommendation 11.

It goes without saying that these retention obligations are extremely costly.[314] All obliged entities are committed to carrying out these measures, and to carrying the burden of cost for their observation. This means that all parties obliged under the anti-money laundering legislation need to cover the costs generated by carrying out identification measures, keeping a system to monitor transactions, sending information on their customers to the local Financial Intelligence Unit, and retaining data safely for long periods of time. The aforementioned costs for lists of politically exposed persons and the expenses in terms of working time are a considerable burden on all financial services providers.[315]

**iv. Risk Assessments**

A new obligation conferred on the obliged entities, Member States, and the European Commission by the fourth Anti-money laundering Directive is to embrace a more comprehensive risk-based approach (article 6-8 4AMLD).[316] The introduction of a risk-based approach is not a classical obligation with which obliged entities are faced, it rather concerns the application of the obligations. Therefore, the risk based approach is not considered a fifth obligation in a line with the four obligations discussed above. As the application of the risk-based approach does have an impact on the four obligations, it should be discussed briefly in this context.

While the earlier versions of the Anti-money laundering Directive applied the rule-based approach, according to which certain rather rigid rules must be applied across the board, it has been recognised that some transactions are more likely vehicles for money laundering and terrorist financing than others.[317] The reason for the introduction of a risk-based approach is that some transactions bear a higher risk of money laundering or terrorist financing, while others are less suitable to be

314 Lennon/Walker (2009), p. 41; Kaetzler (2008), p. 180. See also Kemp (2014), p. 484.
315 See in this context the seventh concern discussed in Chapter IX below, on obliged entites' freedom to conduct a business.
316 See, however, EDPS Opinion 1/2017, p. 12; Kaetzler (2008), p. 175. See also Borgers (2009), p. 149.
317 Sandleben/Wittmann (2010), p. 265; Hamacher (2006), p. 634.

abused for those ends and therefore of lower risk.[318] Those transactions of a higher risk are to be monitored more closely for possible abuse than transactions of lower risk.[319]

The assessment of the risk of any given transaction is based on assessments and typologies compiled and published on different levels. In the first place, on the European level, the Commission will carry out a risk assessment "of money laundering and terrorist financing affecting the internal market and relating to cross-border activities" (article 6 4AMLD). In the second place, measures to identify, assess, research and mitigate risks of money laundering and terrorist financing have to be taken on a national level by Member States (article 7 4AMLD). Lastly, each obliged entity is obliged to "take steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers,[320] countries or geographic areas, products, services, transactions or delivery channels" (article 8 4AMLD).[321] The institutional level is of particular consideration, as it is generally assumed that financial institutions themselves are best capable of identifying the money-laundering risks inherent in their own products and services, and that they can therefore react much more quickly and more efficiently than the law-maker.[322]

Based on these assessments, all business relationships are assigned a risk level. The risk level determines how strict a customer's transactions must be monitored, and which steps must be taken to safeguard against illegal transactions.[323] The obliged entities can, after assessing the risks connected to the services they provide, decide to limit or broaden the extent of the customer due diligence measures applied in each case on a risk-sensitive basis (article 13 (2) 4AMLD).

The risk assessments to be made by the Commission, the Member States and the obliged entities are at the time of writing not yet available. However, there are a number of risk factors prescribed by the Directive, which must be taken

318 Sotiriadis/Heimerdinger (2009), p. 236. See also Amoore/de Goede (2008), p. 176.
319 Sotiriadis/Heimerdinger (2009), p. 236.
320 See in this context also Maras (2012), p. 69. Footnote added by the author.
321 See also Article 29 Working Party Opinion 14/2011, p. 11 on data protection assessments in this context.
322 Kaetzler (2008), p. 175; Lochen (2017), p. 92 f.
323 Kaetzler (2008), p. 175. See in this context also Gellert (2015), p. 3 ff. on the application of risk management in data protection.

into account when assessing risk level of a particular transaction or business relationship, for example the channel chosen, the parties involved, or the countries involved in a cross-border situation.

One factor which can influence the level of risk of a transaction are politically exposed persons.[324] As has already been explained above, politically exposed persons, their family members and close associates are considered high-risk. That the classification of such persons is highly problematic goes almost without saying. The list of politically exposed persons is subject to daily change, and obliged entities lack guidance or an official list of these persons compiled on a European level, forcing them to rely on costly commercial lists,[325] the accuracy of which is impossible for them to verify.

A further influence on the level of risk of a given transaction is the geographic area into which funds are to be transferred or from which they are received.[326] Transactions to and from countries known to have a low level of compliance with international anti-money laundering standards are assigned a higher risk-level for money laundering. Similarly, transactions to and from countries known to have operating terrorist groups in their territory may be regarded as high-risk for terrorist financing.[327]

In this context, it should be noted that the risk-based approach is somewhat departed from in the proposed fifth Anti-money laundering Directive.[328] In recital 19 5AMLD, it is stated that

> "The approach for the review of existing customers in the current framework relies on a risk-based approach. However, given the higher risk for money laundering, terrorist financing and associated predicate offenses associated with some intermediary structures, that approach may not allow the timely detection and assessment of risks. It is therefore

324 See also Maras (2012), p. 69.
325 Kaetzler (2008), p. 177.
326 Kaetzler (2008), p. 178. See also IMF (2005), p. 12.
327 See on the risks of ethnic profiling and discrimination Wensink et al. (2017), p. 151; Article 29 Working Party, Opinion 14/2011, p. 19; Lennon/Walker (2009), p. 41; Maras (2012), p. 73; Favarel-Garrigues/Godefroy/Lascoumes (2011), p. 183 f.
328 See also Article 29 Working Party Opinion 14/2011, p. 10.

> important to ensure that certain clearly specified categories of already existing customers are also monitored on a regular basis".

As the European Data Protection Supervisor notes in this context, "[i]t is not clear on the basis of which criteria, if not risk, such categories of customers will be identified."[329] It remains to be seen when and how this point will be clarified.



Finally, it should also be pointed out that the risk assessment carried out in this context appears to concern almost exclusively factors based on which the risk level, and therefore the customer due diligence measures, must be increased. Corresponding factors which could lower the risk level are largely absent.

## f. Ongoing Developments

### i. The Proposed Fifth Anti-Money Laundering Directive

In July 2016, a little less than a year before the fourth Anti-money laundering Directive entered into force, an update to the framework was already proposed. The fifth Anti-money laundering Directive, still in the process of being negotiated at the time of writing, is to bring a few significant changes to the existing framework.

In the words of *Frans Timmermans*,

> "Today's proposals will help national authorities to track down people who hide their finances in order to commit crimes such as terrorism. Member States will be able to get and share vital information about who really owns companies or trusts, who is dealing in online currencies, and who is using pre-paid cards. Making public the information on who is behind companies and trusts should also be a strong deterrent for potential tax-evaders."[330]

*Timmermans'* words are here quoted as they hint at the motives behind the adoption of the proposal for an update to the existing framework. While terrorism is the first

329 EDPS Opinion 1/2017, p. 12. See also Kaetzler (2008), p. 175; Gellert (2015), p. 15.
330 *Frans Timmermans*, quoted in the European Commission's press release concerning the adoption of the proposal for a Fifth Anti-money laundering Directive.

motive quoted by Vice-President *Timmermans*, it appears to play only a minor role in the text of the proposal. His last mention of the fight against tax evasion would appear to be the leading motive behind the update of the Directive.[331] In the words of *Věra Jourová*:

> "Today, we are putting forward stricter transparency rules to cut terrorist financing and step up our fight against money laundering and tax avoidance. The update of the Fourth Anti-Money Laundering Directive will prevent any loopholes in Europe for terrorists, criminals or anyone trying to play with taxation rules to finance their activities. Better cooperation to fight these issues will make the difference."[332]

There are a number of changes included in the proposal for a fifth Anti-money laundering Directive. One of the most important of these changes is the proposed inclusion of virtual currencies.[333] For this purpose, a definition of the term virtual currencies is to be added, and exchange services and custodian wallet providers are to be included in the list of obliged entities.[334] A detailed discussion of this change is to take place in Chapter IV below.

Secondly, the language of the Directive is tightened overall, closing off potential loopholes, particularly in the description of the tasks of an FIU. These loopholes, which *Ms. Jourová* also mentions, concern for example the fact that some Member States had introduced the rule that an FIU can only request information from an obliged entity on the basis of a prior suspicious activity report submitted by that entity.[335] This option will now be expressly removed from the text of the Directive (article 32 (a) 5AMLD).

The third significant change is the obligation conferred on Member States to introduce central registers for bank account holders.[336] Such registries were

331 See also the fact that the so-called 'Panama Papers' are mentioned in several documents concerning the update of the anti-money laundering framework. See, for example, European Economic and Social Committee 13666/16, p. 6, 8. Critical Sorel (2003), p. 376; Schmidt/Ruckes (2017), p. 473 ff.; Bilsdorfer (2017), p. 1525 ff.

332 *Věra Jourová*, quoted in the European Commission's press release concerning the adoption of the proposal for a Fifth Anti-money laundering Directive.

333 See Chapter IV (c) below.

334 COM (2016) 450, p. 12.

335 COM (2016) 450, p. 13 f.

336 Glos/Hildner/Glasow (2017), p. 87.

already suggested in recital 14 of the fourth Anti-money laundering Directive, but are soon to be obligatory in all Member States.[337] The purpose of such registries is essentially to allow an FIU to identify all accounts held by one person, even if those accounts are kept at different banks.[338] In addition, those registers are to be interconnected on a European level.[339] As the Commission hopes, "[t]his will lead to a faster detection – both nationally and internationally – of suspicious ML/TF transactions, and improve preventive action."[340] The Commission does not, however, bring forth any substantiated reasoning for this confidence.[341] In particular, it should be noted that this approach is not viewed altogether favourably in literature.[342] In particular, the lack of oversight and effective remedies for data subjects have been criticised,[343] and as it has not proven itself very effective.[344]

In addition, there are several changes which play a role of minor importance in the context of this thesis. Those concern for example the adoption of a list of high-risk third countries, which is to follow the FATF's assessment of the risk level of specific countries.[345] Transactions involving those states are to be considered to be of higher risk, triggering stricter due diligence checks to be carried out by obliged entities. Furthermore, the rules concerning prepaid cards are to be strengthened.[346]

**ii. Terrorist Financing**

Apart from the rapid developments concerning money laundering, the rules concerning terrorist financing have also been developed at as rapid a pace.[347] The European lawmaker has concerned itself very much with the fight against terrorism since the events of September 11th, 2001, and especially since the rise of ISIS and the string of attacks in Europe in recent years.[348] A great amount of

337 COM (2016) 450, p. 14. See also Kaetzler (2008), p. 177; Göres (2005), p. 254.
338 COM (2016) 450, p. 14 f. See also recital 14 4AMLD. See also Reichling (2008), p. 672.
339 COM (2016) 450, p. 18. See also Kutzner (2006), p. 640 f.; Krais (2017), p. 98.
340 COM (2016) 450, p. 14; Kutzner (2006), p. 640 f. See, however, also Göres (2005), p. 254 f.
341 See the equal absence of conclusive evidence in the case of the Data retention Directive, pointed out for instance in Leutheusser-Schnarrenberger (2014), p. 590 f.
342 BaFin (2016), p. 62 f.
343 Göres (2005), p. 256 f.; Reichling (2008), p. 672; Hamacher (2006), p. 638. The system of automated screening of bank accounts in Germany has been the subject of a partly successful challenge before the Constitutional Court, see BVerfG 1 BvR 1550/03 [2007].
344 Mack (2006), p. 394; Göres (2005), p. 256 f.
345 COM (2016) 450, p. 15.
346 COM (2016) 450, p. 13. See also Ufer (2017), p. 84.
347 See also Kaetzler (2008), p. 174; Winer/Roule (2002), p. 89 f.
348 COM (2015) 625 final, p. 2 f. See also Waldron (2003), p. 200.

output in Regulations, Directives, and Decisions has been generated. It has been boldly "declared that anti-terrorist finance measures introduced since 2001 have prevented some terrorist attacks",[349] though specific proof for such a claim is not forthcoming. In the meantime, the framework is still in the process of development, with some legislative changes expected shortly. Only the newest and most modern of these instruments are to be highlighted briefly here.

In February 2016, the Commission has communicated an Action Plan on the fight against terrorist financing,[350] and in Mach 2017, the European legislator has passed Directive (EU) 2017/541 on combating terrorism.[351] The Action Plan brings forward a number of different measures, from small amendments of existing laws to large scale innovations to the legal system. The Commission splits its measures into several different types of actions, including the prevention of the movement of funds into the hands of terrorist groups,[352] and preventing terrorist groups from generating revenue themselves.[353] The former is mainly to be addressed by tightening the existing legal framework, particularly the anti-money laundering legislation. The latter is a little more difficult to address, as modern terrorist groups have not only found innovative ways to create revenue, but also ways to commit attacks of unprecedented economy.[354]

Terrorist groups generate revenue using both legal and illegal instruments, particularly through the trade in goods. As the Commission notes,

> "existing EU instruments are not adequate for customs authorities themselves to intervene effectively. Terrorists can gain both from illegal means (e.g. through dissimulation of trade transactions; misrepresentation of the value of goods; fictitious invoicing; or smuggling) and from trade in legal goods. The Commission will consider an explicit legal basis to allow

349 Ryder (2007), p. 847 f.
350 COM (2016) 50 final.
351 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21.
352 COM (2016) 50 final, p. 3 f. See also Basile (2004), p. 175 f.
353 COM (2016) 50 final, p. 12. See also Winer/Roule (2002), p. 89 f.
354 The latest wave of attacks in which an attacker drives a truck into a populated public area is essentially free of financial cost to the attacker. See also Ryder (2007), p. 848; Basile (2004), p. 175 f.

> for provisional detention of goods and for the necessary investigations to be undertaken, notably by FIUs."[355]

In addition, the Commission is concerned about the trade in illegally obtained cultural goods and trafficking of wildlife, which are both utilised for terrorist financing operations, notably by ISIS.[356] Several legal amendments designed to close the loopholes identified by the Commission can be expected in the near future.



## g. Critique

In the previous sections, the anti-money laundering approach was described in some detail. Before concluding this chapter, the major points of critique which may be levelled against this approach should also be discussed, in order to differentiate the perspective provided in this chapter.[357] This section lists not only the points of critique directly connected to privacy and data protection, but will also go briefly into the costs, efficiency and effectiveness of the approach. The critique outlined in this section applies to the anti-money laundering approach currently applied throughout Europe and also beyond its borders.[358]

### i. The Anti-money Laundering Approach

It should be pointed out that that the strategy currently deployed against money laundering and terrorist financing is subject to much strong critique, raised especially in legal literature at national level inside and outside of the European Union. Support for the anti-money laundering scheme has always been meagre at

355 COM (2016) 50 final, p. 12. See also Ryder (2007), p. 825.
356 COM (2016) 50 final, p. 12. See also Ryder (2007), p. 840 f.
357 See for detailed critique among others Hetzer (2002), p. 413; Bures (2015), p. 217 f.; Zeidler (2014), p. 105; Reimer/Wilhelm (2008), p. 240.
358 In this thesis, primarily the approach outlined in the Anti-money laundering Directive is discussed. As has been noted at the beginning of this Chapter, the approach is internationally coordinated under the wings of the FATF. Most countries around the world follow a very similar approach to anti-money laundering, though it is often less sophisticated and less rigorously applied as in the European Union. Therefore, the approach outlined in the previous sections and the critique which is outlined in this section as well as in Chapter IX below, can be applied to all Member States of the European Union and to some extent many countries across the world. The website of the FATF, http://www.fatf-gafi.org/publications/mutualevaluations (last accessed 3 January, 2018) provides information on the anti-money laundering approach followed by each state in the world.

best,[359] and the fight against terrorist financing was fuelled only by the coordinated fight against international terrorism after the events of 11 September 2001. In Europe today, it is universally accepted that laundering dirty money is a crime, and that it should be punished as a criminal offence. However, what is not so universally accepted is how an internationally organised effort against money laundering should be undertaken. The approach currently deployed is widely criticised extensively in literature as an ineffective behemoth of paperwork.[360]

Especially the fact that one approach to anti-money laundering was essentially cast into stone across Europe by a series of detailed directives should be regarded critically.[361] It is true that both money laundering and terrorist financing are crimes which often exhibit international components, and that therefore international cooperation is essential for the success of the approach (recital 4 4AMLD). However, the tight language of the approach outlined in the Directive allows Member States almost no room to differ from the terms of the Directive. There is no space for innovative or experimental approaches to anti-money laundering in order to test whether a more effective approach cannot be found. Room for such experiments and research would be particularly important as the approach currently applied is widely criticised as ineffective.[362] In particular, the vast amount of funds and administrative capacities tied up in the fight against money laundering is not followed by measurable effects,[363] despite continuous amendments to the law, therefore raising doubts as to the justifiability of these expenses. It is not unreasonable to ask whether these resources may not better be applied differently.

In addition, the practice of integrating the financial sector into the tasks of law enforcement should be viewed with some concern. The primary business of financial services providers is, quite naturally, to provide financial services, for which they are paid by customers. The currently applicable approach to anti-money laundering, however, burdens financial services providers with tasks concerning

359 Hetzer (2002), p. 413; De Goede (2008a), p. 176 f.
360 Hetzer (2002), p. 413; Bures (2015), p. 217 f.; Zeidler (2014), p. 105; Reimer/Wilhelm (2008), p. 240.
361 See also Razavy/Haggerty (2009), p. 143 f.
362 Hetzer (2002), p. 413. See also Zeidler (2014), p. 105 f.
363 As shown for instance in Nestler/Herzog, Geldwäschegesetz, 2. Aufl. 2014, § 261 StGB, Rn. 17 ff.

criminal intelligence and national security.[364] This development is being watched with concern by, among others, the European Data Protection Supervisor,[365] and the Council of Europe Commissioner for Human Rights.[366] It will furthermore be seen in the following Chapters V and VIII of this thesis, that the Court of Justice of the European Union has found it necessary to set limits to the utilisation of private sector information by law enforcement agencies.[367]

**ii. The Approach Taken against Terrorist Financing**

The anti-money laundering approach is not the only one being criticised, however. The judgment commonly passed on the approach to terrorist financing is equally harsh.[368] Its effectiveness is disputed at best. Some authors go much further than that, however, stating that "notwithstanding the rhetoric, the war on terror has contributed to the enlargement of the shadow economy and the increase in certain forms of financial crime."[369]

There is also quite some critique voiced in legal literature concerning the application of the same measures to money laundering and terrorist financing.[370] The main points of critique are that terrorist financing concerns often small sums of money which would not raise flags in the day-to-day business of a financial services provider,[371] that cash can be used to extend funds to terrorists, circumventing businesses in the financial sector,[372] and that it is much easier to connect funds to a predicate offence of money laundering than to terrorism,[373] as the majority of these funds are not spent on weapons but on the very ordinary cost of livelihood of the group's members. Finally, it has been pointed out that legislation aimed at combating terrorism in any way "should be kept separate from general crime and security legislation".[374] Due to the severity of anti-terrorism measures, the use of

364 See Casagran (2017), p. 29; Korff (2014), p. 39 f.; Maras (2012), p. 69.
365 EDPS (2013), p. 6.
366 Korff (2014), p. 85 f.
367 Particularly in CJEU Case C-362/14 *Schrems* [2015], paragraph 93, and in CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraphs 57 ff. See in this context also Boehm (2012), p. 341 f.
368 Warde (2007), p. 243 f.; Bures (2015), p. 222.
369 Warde (2007), p. 246.
370 Prominently Roberge (2007), p. 197 ff.; Warde (2007), p. 239.
371 King/Walker (2015), p. 382 f.
372 Wensink et al. (2017), p. 151.
373 King/Walker (2015), p. 384. See also Lavalle (2000), p. 503; Warde (2007), p. 239.
374 Lennon/Walker (2009), p. 40. See also Sotiriadis/Heimerdinger (2009), p. 235; Al-Jumaili (2008), p. 210.

such measures would not be justified in the fight against other crimes, and should therefore not be applied in cases related to crimes other than terrorism.[375]

As has been pointed out earlier, the anti-money laundering legislation is very young compared to other items in criminal law. However, the fight against terrorist financing is an even newer emergence in most countries as well as on the international level. It should therefore not be forgotten that the strategy to combat the financing of terrorism is still "in its infancy."[376] It is not unimaginable that the strategy currently employed, of using anti-money laundering tools for the combating of the financing of terrorism, will be abandoned as a failed first attempt.[377] Indeed, this is not so unlikely, considering that some officials do not hold much confidence that measures against terrorist financing will ever be very effective.[378] One study notes that "even with CFT measures becoming more advanced, terrorists are likely to adopt different methods, such as human couriers, for the exchange and acquisition of money."[379] Ryder considers that "[t]he prevention and detection of terrorist finances is extremely difficult if not impossible, due to the extensive financial tools used to fund terrorist operations."[380] In the words of *Sorel*,

> "it seems that the terrorists' financial machinery has countless resources. To put it plainly, the way their behaviour is able to adapt to and abuse legislation within the framework of laundering in general renders such legislation somewhat redundant, especially in the face of financial and economic globalisation. It is apparent that States have often hesitated to equip themselves with restrictive financial legislation because the law can become an obstacle to the free flow of capital, capital which is indispensable to the economy. This reality remains true today – in the fight against financing of terrorism it is difficult to persuade states that can ill afford to lose vital income."[381]

375 Lennon/Walker (2009), p. 40 f.
376 Sorel (2003), p. 377; Dittrich/Trinkaus (1998), p. 346. See also Winer/Roule (2002), p. 98.
377 Dittrich/Trinkaus (1998), p. 347; Hetzer (2002), p. 413. See also Al-Jumaili (2008), p. 210; Shields (2005), p. 30; Bures (2015), p. 217 f.
378 Bures (2015), p. 222 ff.
379 Wensink et al. (2017), p. 151.
380 Ryder (2007), p. 823 f. See also Leith (2006), p. 107; Al-Jumaili (2008), p. 210; Bures (2015), p. 226.
381 Sorel (2003), p. 377. See also Bures (2015), p. 220.

### iii. Lack of Data Protection Safeguards

Importantly for the subject matter of this thesis, the data protection rules contained in the Anti-money laundering Directive should be briefly mentioned. It is important to note that the first three Anti-money laundering Directives did not contain any references to the applicable data protection framework at all.[382] Neither were the Article 29 Working Party or the European Data Protection Supervisor formally consulted in the law making procedures. Considering the great importance of the role that the analysis and exchange of personal data play in the anti-money laundering framework, this is surprising. This omission was remedied with the fourth Anti-money laundering Directive, which makes several references to the rights to privacy and data protection.[383]

The inclusion of data protection rules is explained in the recitals in the following terms:

> "It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of this Directive and personal data should not be further processed in a way that is incompatible with that purpose.

382 Kaetzler (2008), p. 179; Dittrich/Trinkaus (1998), p. 346. See in this context also Korff (2014), p. 94.
383 COM (2013) 45, p. 11.

> In particular, further processing of personal data for commercial purposes should be strictly prohibited."[384]

The text of the Directive, however, devotes only little space to the discussion of the data protection aspects of the extensive data processing operations to be carried out under the terms of the Directive. While the text of the Directive refers to the Data protection Directive 95/46/EC[385] several times, the content of the provisions concerning data protection are not designed for the protection of personal data. Instead, they are designed in such a way as to exclude as far as possible the rights of the data subject.[386] Article 41 (2) 4AMLD begins with the prohibition that data collected under the terms of the Directive are processed for any other purpose, as is also emphasised in the recital quoted above. However, the following provisions continue to limit the rights of the data subject quite severely. In the first place, as will be explained in detail in Chapter V below, the data subject generally has a right to access data stored about them. While such a right is not absolute and can be limited,[387] such limitations must always be interpreted very narrowly.[388] In article 39 in connection with article 41 (4) 4AMLD, however, the exception becomes the rule: Data subjects may not access personal data because "access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing."[389] There is, however, no support for this blanket statement. While it is true that in some cases, the covert access of data may be essential for the investigation, this should be an exception rather than the rule.[390]

Beyond article 41 4AMLD, there are few provisions concerning the personal data of the customers of obliged entities.[391] The upcoming fifth Anti-money laundering Directive will also not add any further provisions concerning the protection

384 Recital 43 4AMLD. See also recital 46 and 65 4AMLD. See also Kaetzler (2008), p. 179; Hamacher (2006), p. 635; Zikesch/Reimer (2010), p. 97 f. Note that it has been reported that this prohibition is not always complied with, see Frasher (2016), p. 33.

385 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

386 See in this context also Ronellenfitsch (2007), p. 570; Zikesch/Reimer (2010), p. 97.

387 Rawls (2001), p. 104.

388 See also Kielmansegg Graf (2008), p. 23. For historical background, see Donisthorpe (1895), p. 58 ff.

389 Recital 46 4AMLD.

390 See BVerfG, 1 BvR 256/08 [2010], paragraph 243.

391 See in this context also Frasher (2016), p. 17 f.

of personal data. In particular, rules concerning the safe storage of data, the restriction of access to personal data, and the protection of sensitive categories of data are conspicuously absent. The same applies to explicit strict data protection safeguards concerning lists of terrorist suspects,[392] politically exposed persons and their family members and close associates, and registries of beneficial owners. Naturally, the data protection legislation applies to the processing of data under the Anti-money laundering Directive, but some serious conflicts between the two legal documents can already be discerned. These serious conflicts give rise to seventeen concerns connected to the anti-money laundering approach.

**iv. Concerns**

A close examination of the anti-money laundering measures shows that the approach chosen by the regulators against money laundering depends to a large extent on data processing operations. Data processing operations on a large scale such as this are the very reason for the existence of data protection legislation. The privacy and personal data of data subjects are to be safeguarded against the various threats inherent in such data processing.[393]

The four duties of identification, monitoring, reporting, and data retention are all connected to a number of data protection and privacy concerns. While those concerns build upon the remarks which will be made in Chapters V to VIII below and will be elaborated upon in detail in Chapter IX, they may already be briefly mentioned in this context.

In the first place, it may be argued that the mass surveillance character[394] of the anti-money laundering measures is altogether too far-reaching. Such an argument would be based on the sweeping character of the measures, and on the lack of exceptions for either persons or categories of transactions. Secondly, and closely related, some obliged entities may be covered by the Directive whose relationship

392 Bergles/Eul (2003), p. 278 f.

393 See for these threats Koops (2014), p. 256.

394 As Privacy International (no date) put it, "Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring." The concept of mass surveillance has not yet been introduced, but will play a major role in the following sections. The concept is first explored in detail in Chapter V, section e, and the mass surveillance character of the anti-money laundering approach is subject of the first concern discussed in Chapter IX. Furthermore, the (cumulative) proportionality of measures of mass surveillance will be the subject of Chapter X below.

with their clients are protected by professional secrecy under national law. The exception for lawyers contained in the Directive is very narrow, and it may be questioned whether it is not too narrow to grant meaningful protection to the confidential relationship between a lawyer and a client.

The identification duties are a third point which one may be concerned about, specifically the lack of exceptions and the resulting lack of situations in which financial services may be used anonymously. Anonymity is, however, as will be explained in Chapter VII, the best safeguard for a thorough protection of a data subject's privacy.[395]

The surveillance of transactions carried out by obliged entities also raise a number of concerns. A fourth concern would be that obliged entities are monitoring a customer's transactions in order to detect suspicious activity, but as has been mentioned, the definition of suspicious transactions is entirely unclear. In the fifth place, the reader can imagine that some financial transactions are of a particularly private nature and contain personal data falling into the category of sensitive data.[396] Safeguards for sensitive data are, however, absent from the text of the Directive. Furthermore, the monitoring duties comprehensively affect all customers of the financial services industry, although the majority of them cannot by any stretch be considered to be suspects of money laundering or terrorist financing. It may legitimately questioned whether levelling measures against such individuals is not in conflict with the principle of the presumption of innocence. Regarding the monitoring duties from another angle, it can in the seventh place be questioned whether the costs involved in the monitoring do not cause a conflict with the service provider's freedom to conduct a business.

The reporting of suspicious transactions also raises a number of concerns. The eighth and ninth concerns in this context are connected to the exchange of information between the obliged entities and FIUs: the duty to report all suspicious transactions is a concern, and the duty to comply with requests for information

395 Both the benefits of anonymity for the privacy of individuals, as well as the risks of anonymity connected to criminal activity are discussed in Chapter VII below.

396 Sensitive data is information falling into categories of personal data which is considered particularly sensitive by the lawmaker, often due to the close connection between certain information and discrimination. Article 9 (1) GDPR protects for instance information revealing the ethnic origin or sexual orientation or data subjects. See for a detailed discussion of sensitive data Chapter V (d) below.

is also a concern. Both concerns are increased by the fact that the customer is not notified of the disclosure of personal data to the FIU. The prohibition of disclosure is a tenth item which may be viewed with concern. Closely connected is the eleventh concern, which is that the data processing operations carried out under the Directive are marked by a general lack of transparency, which, in the twelfth place, may obstruct the data subject's right to an effective remedy in the event that processing of personal data was unlawful.

Additionally, the retention of data is also an obligation which raises a number of concerns. The thirteenth concern is raised by the lack of data protection safeguards to ensure the security of the retained customer data. In addition, and as a fourteenth point, the proportionality of the length of the retention period may be questioned. Business relationships may be of some duration, which may result in a retention period of several decades. Furthermore, the data collected and retained under the Directive is slowly being utilised for other purposes than the fight against money laundering and terrorist financing. In this way, access to data was granted to tax authorities. This access by tax authorities is the subject of a fifteenth concern, and a sixteenth concern would be raised by the apparent departure from the principle of purpose limitation in general.

Finally, in the seventeenth place and in view of the future, some of the measures which have been proposed in the fifth Anti-money laundering Directive raise concerns. In particular, the proposed databases of bank account holders and a potential database of users of virtual currencies[397] are developments which may be observed with concern.

The reader will already have spotted some of these concerns while reading the analysis of the anti-money laundering measures above. However, before going into additional detail concerning these issues, the theoretical framework within which they will be evaluated must be constructed. Deeper discourse on the data protection legislation and the principle of proportionality will be the subject of Chapters V and VIII below. A detailed account of potential conflicts between the anti-money laundering measures and the rights to privacy and data protection is the subject of the main research question. The research question will be answered after a detailed discussion of these seventeen concerns in Chapter IX below.

397 See Chapter IV (c) below.

## h. Conclusion

The European legal framework concerning anti-money laundering and terrorist financing is thus in fact made up of a series of legal innovations conceived mainly in Europe and North America since the 1970s and implemented globally, evolving rapidly into the finely meshed system of identification, monitoring and reporting duties it is today. The rapidity with which this field of law evolved is unprecedented,[398] and with the fifth Anti-money laundering Directive currently passing through the law-making procedure, there are still more developments ahead.[399]

The anti-money laundering framework in principle consists of a number of obligations conferred upon obliged entities. Obliged entities are in the first place all institutions and businesses that together make up the banking sector, and in the second place other professions that have been identified either as vulnerable to money laundering operations, such as real estate agents, casinos, or members of the legal professions.

As has been shown, the obligations conferred upon those entities are fourfold. In the first place, obliged entities must identify all of their customers, and verify the identity. This includes also legal persons, in which case obliged entities must identify the beneficial owner ultimately standing behind the legal person. Secondly, the transactions of each customer must be monitored in order to be sure that the services of the obliged entity are not being abused for the purposes of money laundering or terrorist financing operations. In case any transaction raises suspicions of money laundering or terrorist financing, the obliged entity must thirdly report this transaction to the FIU and comply with potential requests for additional requests for information. The customer cannot be notified of such a report.[400] Finally, the obliged entity must retain customer data for five years after the end of the business relationship, or longer, if national law extends the retention period.

398 Warde (2007), p. 240.
399 Allaire (2013), p. 116 f.
400 See also Boehm/De Hert (2012), p. 4.

In conclusion, it must be emphasised that the anti-money laundering measures are very far-reaching, and that they introduce a sweeping system of identification, transaction monitoring, reporting, and data retention. This system has some obvious points of collision with the human rights to privacy and data protection, which are the pivot of this thesis and the subject of the seventeen concerns discussed in Chapter IX.

The following chapters will build upon the analysis of these obligations. While essential points concerning the obligations and the obliged entities will be repeated where necessary, the reader may wish to refer back to this chapter over the course of the thesis to refresh their memory in specific points. The following chapter will begin to expand upon the point of obliged entities, adding alternative transactions systems to the picture.

# Chapter III

## Understanding Alternative Systems for Financial Transactions

## Outline:

a. Introduction
    i. "Underground Banking"
    ii. Adding Alternative Transaction Systems
b. The Conventional Banking Sector
    i. Definition
    ii. Organisational Features
    iii. Who uses the Conventional Banking Sector?
    iv. Implication in Financial Crime
c. Cash
d. Virtual Currencies
    i. Definition
    ii. Development and Technical Issues
    iii. The Blockchain
    iv. Miners and Cryptography
    v. Third-Party Services in the Virtual Currency Environment
    vi. Who uses Virtual Currencies?
    vii. Implication of Virtual Currencies in Financial Crime
e. Informal Value Transfer Systems
    i. Remittances
    ii. History and Development
    iii. Definitions
    iv. How it Works
    v. Structure of the Network and Record Keeping
    vi. Statistics
    vii. Who uses Hawala?
    viii. Advantages of Hawala
    ix. Sharia Compliance
    x. Implication of Hawala in Terrorist Financing
    xi. Implication of Hawala in Money Laundering
    xii. Resistance to Regulation
f. Conclusion

## a. Introduction

### i. "Underground Banking"

Roughly, the financial transactions market can be split up into two major categories. That is in the first place the regulated banking sector, including credit institutions but also credit card companies, official remittance services and online money transmitters such as *pay pal* and *iDeal*. The second category comprises the sum of unregulated channels commonly collectively called 'underground banking', or 'shadow banking',[401] including the Hawala network, virtual currencies and other channels which, for different reasons, easily elude attempts at regulation from national governments.

Virtual currencies are a relatively new phenomenon, the most prominent examples for which are Bitcoin and other systems, which are variations ('forks') based on the open source Bitcoin protocol. Virtual currencies are financial services systems, usually including an original unit of account, that operate entirely online and are often secured through and based on cryptography.[402] Virtual currencies are radically different from the traditional banking sector because they are not linked to a large central entity as a bank, but are based on a loosely knit network of users running the same code on their computers, and a ledger of all transactions ever accomplished through the system, which is accessible to all users for reference.[403] Virtual currencies can also be used for remittances,[404] if the necessary technological infrastructure is present with both the sender and the receiver.

Informal value transfer systems are the second group of channels to be examined here under the term 'underground banking'. Remittance systems are channels for financial transfer that offer migrants a possibility to send a portion of their wages to friends and family members in their country of origin. There are regulated services that specialize in remittances, such as *Western Union* and *MoneyGram,* but there are also systems that operate without compliance with the applicable laws, thus underground. One of the major channels for remittances underground is Hawala. Hawala is a transfer system which allows for informal financial transfer with very wide reach, low thresholds, and for the most part withdrawn from official

401 Ryder (2007), p. 825; BMF (2004), p. 80 f.
402 Sorge/Krohn-Grimberghe (2012), p. 484.
403 Hildner (2016), p. 488.
404 Murck (2013), p. 94 f.

oversight. These factors make it at once virtually indispensable for the migrant community, but also vulnerable to abuse.

**ii. Adding Alternative Transaction Systems**

In this Chapter, alternative transaction systems are to be introduced and added to the scope of this thesis. The alternative transaction systems to be discussed in this thesis are informal value transfer szystems, of which Hawala is the main representative,[405] and virtual currency systems, for which Bitcoin is chosen as representative.[406]

In recent years, both informal value transfer systems and virtual currencies have received an increased share of public attention. At this point, most people who follow the financial and technical news will have heard of both Hawala and Bitcoin, the most well-known representatives of each system, especially in connection with financial crime and terrorism. But what kind of system stands behind those terms, and how either system precisely works, is not at all widely known.

Virtual currencies and the Hawala network are the subject of studies in many different fields of science. Virtual currencies are not only of interest in the field of law, but also in computer sciences, economics, and social sciences. Indeed, aside from the obvious interest generated in the field of computer sciences, there appears to be more interest in virtual currencies in economics than in law, in which discipline virtual currencies are only slowly beginning to be considered.[407] Hawala in contrast is being studied extensively in social sciences and history, while there are only very few recent sources in law dealing with Hawala, even fewer that have been published in Europe.

405 As will be explained in more detail in section (e) below, there are many different informal value transfer systems. Hawala was chosen as representative because it is one of the biggest, if not *the* biggest system in terms of moved value and worldwide accessibility, and because information on it is most readily accessible.

406 Bitcoin was chosen as a representative for all virtual currencies, because it is best-known and until now most widely used, because it was the first successful virtual currency, and becuase the majority of other virtual currencies was based on the Bitcoin protocol.

407 See in this context also *Cohen's* comment on "the general backwardness of legal science", in Cohen (1935), p. 830.

This chapter is intended to explain in detail both informal value transfer systems, the most prominent system being the Hawala network, and virtual currencies, the most prominent system being Bitcoin. Further light will be shed on how they are used to transmit value, and how wide-spread the use of each system is. This chapter is therefore the introduction of those alternative systems, the basis upon which their assessment in all following chapters is built. It will also answer the sub-questions to the main research question that concern alternative transactions systems, namely what they are and how they function. The background given on those systems may punctually go beyond what is strictly necessary for a reader to follow the arguments made in later chapters. It is likely, however, that this chapter is for many readers a first acquaintance with these systems. A full picture was, therefore, deemed necessary in order to enable readers previously unfamiliar with one or both of those two systems to gain a thorough understanding of them. For this purpose, this chapter will also largely omit a legal discussion at this point. An assessment of how the systems fit into the anti-money laundering framework will then be the subject of Chapter IV.

Both virtual currency systems and informal value transfer systems are particularly interesting from the perspective of privacy and data protection. While this aspect will not be discussed explicitly in this chapter but in Chapters VI and VII as well as Chapter IX section (j) below, the remarks made in this chapter are the basis upon which the privacy and identity issues connected to these two systems will be discussed in the later chapters. Identity issues come into play whenever an individual chooses an alternative transaction system over the conventional banking system. There are many different reasons for such a choice. These reasons are going to be discussed in the present chapter; the connection to the identity of users is made and elaborated upon in Chapter VI. Privacy issues are also of particular interest. Both of the alternative transaction systems discussed in this thesis are related to a number of privacy advantages and risks. Based on the initial explanations of the privacy issues related to both systems and the further discussion of these issues in Chapters VI and VII, Chapter IX section (j) will discuss the question whether alternative transaction systems may provide increased privacy to its users compared to the conventional banking sector.

This chapter is structured as follows: after the introduction, the main features of the conventional banking sector are to be outlined in section (b), and cash is to be introduced in section (c). This explanation of the features of the conventional

banking system is to serve as a basis of comparison for the following introduction of alternative transfer systems, namely virtual currencies in section (d) and informal value transfer systems in section (e).

## b. The Conventional Banking Sector

### i. Definition

It may be assumed that all readers are familiar with the regulated banking system prevalent in Europe, and so the outline of this system will be only brief to serve as a standard against which to compare alternative systems. The very large majority of international financial transfers are processed by the conventional banking system.[408] The most prominent channels are giro transactions, payments made by direct debit, and cheque transactions.[409] The volume of transactions, both in terms of quantity and value, and the involvement of banks in all areas of the European commercial system, interacting with the national governments and businesses as well as the consumer, have caused the growth of a detailed system of financial regulations, covering almost every aspect of the work of banks in Europe. A few of these will be explained in detail and continually referenced hereafter.

The *Oxford English Dictionary* lists several definitions for the word 'bank'. The most insightful of those definitions defines a bank as "[a]n institution that invests money deposited by customers or subscribers, typically pays interest on deposits, and usually offers a range of other financial services, including making payments when required by customers, making loans at interest, and exchanging currency; a building occupied by such an institution."[410] This definition essentially covers the notion of a credit institution as applied by the Anti-money laundering Directive. A service provider offering not all but specialising in only one or more of the tasks mentioned in the definition is a financial institution under the terms of the Directive.

The definition of a bank to be applied for the purposes of this thesis is that of the credit institution, to be found in the Anti-money laundering Directive. Credit

408 Knops/Wahlers (2013), p. 240.
409 Knops/Wahlers (2013), p. 240.
410 Oxford English Dictionary, Third Edition 2010, s.v. "Bank".

institutions are defined as "a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council, including branches thereof, as defined in point (17) of Article 4(1) of that Regulation, located in the Union, whether its head office is situated within the Union or in a third country" (article 3 (1) 4AMLD).[411] Point (1) of Article 4(1) of Regulation 575/2013 then clearly defines a credit institution as "an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account", and a branch of such a credit institution is defined in point (17) of the same article as "a place of business which forms a legally dependent part of an institution and which carries out directly all or some of the transactions inherent in the business of institutions".[412] This definition very much coincides with the definition found in the dictionary and with the concept most people will have of the conventional banking sector in Europe today.

For the purposes of the following thesis, all undertakings will be considered part of the conventional banking sector, which establish a more or less permanent business relationship with the customer, usually in the shape of an account, and which process transactions for the customer in an open system. The further activities of banks are less relevant for the purposes of this thesis, which will focus almost exclusively on transactions. In addition, the conventional banking sector also includes financial institutions which do not offer the comprehensive service of a bank but rather specialise in a certain field. Therefore, most retail banks as well as credit card companies, currency exchanges, and services such as *pay pal* and *iDeal* should be considered as examples of the conventional banking system. The reason for this very wide definition is the fact that the focus of this thesis lies on the particular features of an institution to which the anti-money laundering legislation primarily connects, which is the processing of customer data and transaction data.[413] The other remaining economic services offered by a bank offer

411 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–117.

412 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 Text with EEA relevance, OJ L 176, 27.6.2013, p. 1–337.

413 Müller/Starre (2014), p. 23 f.

great distinctions between the different types of banks, but are not of interest in this thesis.

**ii. Organizational Features**

In the interest of allowing a proper distinction between the banking sector and virtual currencies and informal transfer systems, it is necessary to point out some rather obvious features of the banking system. The average bank in Europe today is likely to be properly licensed, registered, and incorporated somewhere in the world, and may have branch offices in many different cities and Member States. There are generally offices, employees, an extensive technical infrastructure, and a considerable interest in consumer goodwill and the corporate image cultivated by the institution.

It is important to realize that banks are generally centrally organized constructions. The system allows a customer to store funds in his or her bank account, and when a request for the movement of funds is made, the bank is in charge of moving the funds to or from the customer's account. It will be seen that this is a stark contrast to the decentralized networks of virtual currencies and informal value transfer services.

The inner workings of a bank are as a black box to many people, so an example may serve at this point to offer a simplified illustration of the involvement of banks in financial transactions carried out through their services.[414] When carrying out an electronic transaction, a customer can log into his or her online banking account, and carry out a financial transaction him or herself. For instance, in order to pay the rent, the customer of a bank can log into his account, enter the account information of his landlady, and specify the proper amount. After security verification, the customer's task is completed. The bank is then responsible for transmitting the funds. If both the customer and his landlady have accounts with the same bank, the bank can very easily move the funds between the two accounts. Therefore, while the transaction is nominally between the customer and his landlady, the bank is needed as a third party responsible for the actual movement of the funds. If the landlady has an account with another bank, the system becomes a little more complicated, because the customer's bank has to communicate with the landlady's bank in order to facilitate the move of funds from one account to the other. Therefore, the transaction between the customer and his landlady in this

414 See also Geva (2016), p. 285 f.; Eichler/Weichert (2011), p. 202 f.

case involve four parties in total, as the involvement of both banks is needed to process the transaction. If either the customer or the landlady have an account with a bank in another Member State or even a third country outside of the European Union, the amount of parties involved in the transaction may increase to five or more, as often an external service is involved in order to facilitate the cross-border movement of the funds.



Therefore, it should be noted that an online transaction, which initially appears to be directly between two persons, may involve a number of third parties to take place. Therefore, the only conventional means to carry out a financial transaction directly between two people is to use cash, which can be handed over from one person to another directly.[415]

### iii. Who uses the Conventional Banking System?

The *Worldbank's Global FinDex* 2014 estimates that 62 percent of all adults worldwide are owners of a bank account.[416] The global nature of this number demands some clarification, however, as the numbers will be widely different between a European country and the rest of the world. In most countries in Europe, the conventional banking system is ubiquitous. Almost the entire population is covered by the conventional banking system, meaning that every inhabitant should at least have access to a bank account, if not to other services commonly offered by banks.

There is, however, a small percentage of persons in Europe who are considered 'unbanked', meaning that they do not have access to this basic banking service. Estimating this percentage is naturally very difficult, but it is generally placed at 7 percent[417] for the entire European Union, with rather large differences between the individual Member States. For instance, it is estimated that only half of the population in Bulgaria and Romania have access to a bank account,[418] while the coverage in Denmark and Finland is estimated to be at 100 percent.[419] However, it should be pointed out that undocumented immigrants are generally not taken into account when these estimates are made.

415 See section (c) of this chapter below.
416 Global Findex 2014, p. 11, available at http://www.worldbank.org/en/programs/globalfindex (last accessed 3 January, 2018).
417 European Commission, SEC(2011) 907, p. 1. See however Datta (2009), p. 331, for numbers of the unbanked migrant population.
418 European Commission, SWD(2013) 164 final, p. 24.
419 European Commission, SWD(2013) 164 final, p. 24.

The reasons for the lack of access to banking services in some Member States are varied.[420] Very poor, indebted, and homeless persons are largely excluded from the banking system due to their lack of creditworthiness. Furthermore, elderly persons in rural and underdeveloped regions of Europe are also more likely to be unbanked or underbanked. Finally, undocumented immigrants are generally excluded from accessing official banking services, as they lack official documents used for identification.[421]

The interest in helping unbanked persons to gain access to the conventional banking sector has been taken up by the legislator. The first two groups of persons vulnerable to financial exclusion as mentioned above are, therefore, aided by the new Payments Accounts Directive 2014/92/EU,[422] which aims to grant access to a bank account with the most basic features to all inhabitants in the European Union. The latter group of persons vulnerable to financial exclusion, undocumented immigrants, are not going to be aided by this Directive, as it only paves the way for access to bank accounts for legal residents. Undocumented immigrants do not meet this condition and are therefore excluded. This omission is especially noteworthy as the number of undocumented immigrants in the European Union could be very high. The exact number is difficult to estimate, but in 2014, the number of persons found to be residing illegally in the European Union was 626 thousand persons.[423] Those are certainly only the established cases. The number of undetected cases is nearly impossible to estimate with any degree of certainty, but all sources do agree on the number being very high. For instance, the German secret service estimates that 15-20% of all migrants could reside in Europe illegally.[424] It is important to keep in mind that this large number of persons is not considered in the statistics, but that those people naturally must use some sort of alternative banking services if they are excluded from the services of the conventional banking sector. The Hawala system often provides services to these individuals.

420 European Commission, SWD(2013) 164 final, p. 23 f. See also Murck (2013), p. 94 f.
421 See in this context also Mezzana/Krlic (2013), p. 5.
422 Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, OJ L 257, 28.8.2014, p. 214–246.
423 See the statistics at http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_enforcement_of_immigration_legislation (last accessed 3 January, 2018).
424 See http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Migration/Migration_node.html (last accessed 3 January, 2018).

**iv. Implication in Financial Crime**

Naturally, the sheer size of the banking industry makes it an ideal tool for the purposes of financial crime. The United Nations Office on Drugs and Crime estimates that ca 2-5% of the global GDP is laundered each year.[425] More specific figures are calculated by the FATF, which estimates that in 2009, 3.6% of the global GDP was of criminal origin, and that 2.7% of the global GDP was going through money laundering.[426] The figure on money laundering translates to 1.6 trillion US dollar. Naturally, those are the numbers of money laundered through all channels. However, if one connects this number to the fact that almost all legal residents of the European Union are connected to the conventional banking system, it becomes reasonable to estimate that most of the money laundering operations carried out in Europe involve the conventional banking system at some point.



The conventional banking system is at once the primary financial service provider for residents in the European Union and the primary instance involved in the detection and reporting of money laundering schemes. The majority of suspicious transaction reports are filed by banks. For instance in Germany in 2016, 86% of all suspicious transactions reports were sent by credit institutions, and that number rises to 99% when financial institutions are added.[427] Of course, the amount of suspicious transaction reports does not necessarily reflect the true size of criminal activity facilitated by the conventional banking sector. However, the amount of suspicious transaction reports does reflect the greater danger for persons involved in financial crime to be discovered. This naturally creates an incentive to move on to transaction systems in which the service provider is not vested with a large compliance department scrutinizing each and every transaction, such as virtual currencies and informal value transfer systems. Most prominently, however, cash is used in those cases.

## c. Cash

In order to cover all means used for financial transfers, and as it will be relevant in the following sections, cash must briefly be mentioned separately. Cash is "[m]

425 UNODC (no date).

426 See The FATF, http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223 (last accessed 3 January, 2018).

427 FIU Jahresbericht 2016, p. 10; Müller/Starre (2014), p. 24. See also for the similar situation in the United Kingdom NCA annual report 2015, p. 10 f.

oney; in the form of coin, ready money."[428] Cash therefore means the coins and banknotes used as a medium of exchange, universally applicable to complete a transaction directly between two persons.[429]

Cash can take one of two different shapes: fiat and commodity.[430] Commodity money has an intrinsic value, such as coins minted in gold and silver.[431] The value of the money is thus directly tied to the value of the precious metal in the coin. Fiat money appeared later than commodity money and is now the predominant type of currency in use in the world. Fiat money is issued by the government of a country to serve as the legal tender in that country, but the token designated as money has little intrinsic value in itself.[432] In this way, most fiat currencies are made up of paper banknotes, and of coins that are minted in metals of low value. Fiat currency can also easily be represented digitally. One of the main features of fiat currency is that only the fiat currency of a particular country will be accepted by the government of that country for the payment of taxes.[433] This circumstance makes the fiat currency of a country indispensable to any inhabitant of that country, as taxes cannot be valued or paid by any other medium.

Fiat currency can take the shape of hard cash in coins and banknotes, and that of e-money, which is a virtual representation of currency used in virtual transactions, such as the transfer of money using an online banking service, or payment by credit card. However, in contrast to such transactions, hard cash is an anonymous means of financial transfers.[434] In a great majority of transactions, cash is exchanged between two persons who will not be personally known to one another. For instance, a five euro bill may be used by a customer to buy an item from a supermarket. The cashier may routinely check the genuineness of the banknote, but if the note is genuine, there will be no reason to identify the customer, as the transaction is completed with the exchange of the banknote for the goods. This same banknote may be handed to another customer as change in a following transaction. This customer will not know who the previous owner of that note was. When the bill is next spent, the customer may already have forgotten where and when exactly he has received it. These details are not recorded nor remembered

428 Oxford English Dictionary, Third Edition 2010, s.v. "cash".
429 Söllner (2009), p. 3340. See also Anderson (2014), p. 428 f.; Kubát (2015), p. 410.
430 Filippi (2014), p. 5. See also Wolf (2016), p. 233 f.; Kant (1887), p. 125 f.; Mill (1821), p. 92.
431 Hunter (2014), p. 1.
432 Hunter (2014), p. 1; Söllner (2009), p. 3340.
433 Hunter (2014), p. 1. See also Elias (1982), p. 207 ff.
434 Fan/Huang (2010), p. 567.

or attended to, because the transaction is completed when the physical banknote or coins have changed hands, and because the identity of the banknote or coin is not of the essence; it is solely the value of the notes or coins which is of interest to the parties.

While bank notes are marked with unique serial numbers, these numbers are highly impracticable to be tracked by any other party than an established bank.[435] An average banknote of a small denomination will travel through many hands before it is turned back to a bank, and none of the parties by whom it is used for a transaction will typically have noted the serial number.



Therefore, cash is the only means of financial transaction discussed in this context, which is completely anonymous.[436] This anonymity especially comes into play when looking at Hawala transactions, which rely on cash, and to some extent specifically on the anonymity of cash, as will be seen in the following sections.

Finally, the digital representation of cash should be mentioned briefly. This digital cash is called *e-money*. E-money is "a digital representation of fiat currency used to electronically transfer value denominated in fiat currency."[437] E-money is thus fiat currency in digital form, rather than in coins and banknotes, for the purpose of electronic banking. This way, the conventional banking sector offers many payment services online, using digital representations of euros, pounds, or dollars, but the structure of the system is still that of the conventional banking sector, and not, as will be seen below, comparable to a virtual currency.

## d. Virtual Currencies

### i. Definition

Commodity money has been in use for thousands of years, and fiat currency has been used for several hundred years. Virtual currencies have only been in use since 2009, and are neither fiat nor commodity money,[438] as they lack any physical

435 See in this context Recommendation No. R(80)10 of the Committee of Ministers to Member States on Measures against the Transfer and the Safekeeping of Funds of Criminal Origin. Adopted by the Committee of Ministers on 20 June 1980 at the 321st meeting of the Ministers' Deputies.

436 See, in this context, also Simmel (1906), p. 467; Rossum et al. (1995), p. 41 f.

437 FATF virtual currencies (2014), p. 4. See also Vardi (2016) p. 61 f.

438 Filippi (2014), p. 5; Wolf (2016), p. 233 f.; Kubát (2015), p. 410.

representation,[439] and are generally not created by any government.[440] A virtual currency is indeed not a 'currency' at all, in that it is not issued by a national central bank and no jurisdiction guarantees for its value.[441]

There are different definitions of virtual currencies. The FATF has published a definition according to which a "virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction."[442] The European Commission has lately become active in the field of virtual currencies, and proposed the following, very similar definition: "'virtual currencies' means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically".[443] The definitions accurately make it clear that virtual currencies are currencies which only exist online and are not issued by a central bank or any similar authority.[444]

The vagueness of the two definitions of virtual currencies is largely caused by the nature of the technology: It is still being developed, and there are hundreds of different virtual currencies which do not all function in the same way. In the first place, there are open (convertible) virtual currencies, and there are closed (non-convertible) virtual currencies. Open virtual currencies can be exchanged for fiat currency and is traded against a dynamic market value, while closed virtual currencies are only used on a particular online platform, such as a gaming platform or an online shop.[445] Secondly, there are centralized and decentralized virtual currencies. Centralized virtual currencies are usually non-convertible, as they

439 In fact, some virtual currency units of Bitcoin have been minted in a physical form by early adopters, and images of those minted bitcoins are often used in stock photos. The exchange of one minted coin does not, however, transfer the value of a bitcoin in itself, as those can only be moved virtually on the blockchain. Therefore, the few minted representations of bitcoin should be entirely disregarded in this context.

440 Some national virtual currency projects have been undertaken, with varying degrees of success, in, among other countries, Iceland, Spain, and Cyprus. See Gilbert (2014).

441 FATF virtual currencies (2014), p. 4. See also ECB Opinion 13303/16, p. 3; Beck (2015), p. 580 f.; Bonaiuti (2016), p. 36.

442 FATF virtual currencies (2014), p. 4. See also Beck (2015), p. 581; Anderson (2014), p. 428 f.; Sorge/Krohn-Grimberghe (2012), p. 484.

443 COM (2016) 450, p. 30.

444 Shasky Calvery (2013), p. 49 f. See also Vardi (2016) p. 59 f.

445 FATF virtual currencies (2014), p. 4.

are issued by a specific entity for the purpose of carrying out transactions on the online platform of that entity. In contrast, decentralized virtual currencies (often also called *cryptocurrencies*) are virtual currencies based on cryptography, whose systems are distributed via a peer-to-peer network among users worldwide.[446]

The type of virtual currency which is examined in this thesis is the open and decentral variation, based on cryptography. The main example of this type of virtual currencies is Bitcoin, but there are several hundred systems now in existence, with varying degrees of popularity. This type of virtual currency is a very interesting phenomenon, because it allows for the widest applicability and offers the greatest contrast compared to the banking system.



**ii. Development and Technical Issues**

The virtual currency which is currently generally best-known, has the largest userbase and receives the most media attention is Bitcoin. Because Bitcoin was the original protocol that first started the global rise of open systems of virtual currency, because most other virtual currencies in circulation today are based on the Bitcoin system, and because it is the system with the largest following worldwide, Bitcoin will largely stand as a representative for the sum of other virtual currencies hereafter.

The introduction of the Bitcoin system is preceded by considerable history. Bitcoin and its forks are some of the newest links in a rather long chain of experimentation with cryptography for the purpose of creating virtual currencies. Since at least 1985, cryptographers had been toying with ideas for cryptocurrencies, but each system that was proposed was soon again discarded because of technical flaws.[447] Finally, in 2008, a white paper called "Bitcoin: A peer-to-peer electronic cash system" by a programmer calling himself *Satoshi Nakamoto* was circulated via a cryptography mailing list. Until today, it is not known which person or group of persons stands behind this pseudonym, although many different theories have been developed.[448] After launching the project in the beginning of 2009, *Nakamoto* remained in

446 FATF virtual currencies (2014), p. 5; Murck (2013), p. 91; Tschorsch/Scheuermann (2016), p. 2085.

447 *Jeong* (2013), p. 9 f.; see also Holznagel/Tabbara (1998), p. 391 f. See in this context also Diehl (2008), p. 243 f.

448 See *Davis* (2011) for a list of theories that were developed and abandoned around the identity of Satoshi Nakamoto. See also Raman (2013), p. 66 f.

e-mail contact with a few developers in order to iron out some difficulties with the code, but disappeared after several months and is now not to be found.

The most difficult challenge in earlier proposed virtual currency schemes was to find a solution to the 'double spending problem'.[449] Computer files can generally be copied and shared numerous times, while the original copy remains undiminished on the user's PC. If the unit of account in a virtual currency, for instance one bitcoin, is a computer file and can be sent to numerous transaction partners for different transactions, the system would disintegrate instantly. Therefore, in order to be secure, a system has to be endowed with extensive security features that prevent people from tricking the system into accepting the same unit twice. No proposed decentralized system before Bitcoin had a level of security that would make it safe enough for implementation as a financial transaction system.

The difference between Bitcoin and the earlier proposals for virtual (crypto-) currencies is that by using an open peer-to-peer infrastructure as a basis, *Nakamoto* designed a system without the need for a central authority that oversees the administration of the system and through which all transactions would be routed. Furthermore, all transactions are openly accessible for everyone and recorded in a ledger (the *blockchain*), and are verified by other users instead of a central authority.[450] These three features, the peer-to-peer infrastructure, the lack of a central authority, and the open accessibility of the blockchain are crucial points in the Bitcoin protocol and architecture.

Thus, basically, Bitcoin is a technology that establishes a currency without the need of an overarching central authority that controls it and through which transactions would be routed. Instead, it uses a peer-to-peer network which allows the community to assume the role that would otherwise be fulfilled by the bank. It thereby provides an alternative for financial transactions,[451] allowing users to circumvent the traditional banking sector.

449 Kütük/Sorge (2014), p. 643; Rückert (2016), p. 6; Tschorsch/Scheuermann (2016), p. 2093.
450 Murck (2013), p. 92 f.; Rückert (2016), p. 6; Tschorsch/Scheuermann (2016), p. 2085 f.; Simmchen (2017), p. 163.
451 Murck (2013), p. 92 f.; Anderson (2014), p. 429 f. See also correctly CJEU C-264/14 *Hedqvist* [2009], paragraph 24.

The term Bitcoin refers to both the entire infrastructure, which is the Bitcoin system or protocol, and the unit of account.[452] The virtual currency Bitcoin is measured in bitcoin, just as fiat currencies like the euro or the dollar. In order to differentiate between the two terms, the unit of account is usually spelled with a lower case b, and the system's name with an upper case B. Each bitcoin is divisible into eight decimal places, which ensures that each fiat currency can be exchanged with a sufficient degree of exactness.[453] The smallest unit into which a bitcoin can be divided is called a 'Satoshi', named in honour of *Satoshi Nakamoto*. One Satoshi is 0.00000001 Bitcoin, or the other way around, 100,000,000 Satoshi add up to one Bitcoin.

Bitcoin can be acquired by anyone either by exchanging fiat money for Bitcoin, usually through an online exchange, or by receiving bitcoin from other users, for example as a payment for goods and services. Miners also acquire bitcoin in the course of their work.

**iii. The Blockchain**

Each user has access to the blockchain, which is a public ledger that records every transaction ever carried out over the system, starting with the first block ever mined (the *genesis block*), and chronicling all transactions until the most recent one carried out.[454] The blockchain is crucial for the architecture of the system. As one of Bitcoin's main design features is the decentralization of the system, there is no central authority which carries out the tasks ordinarily carried out by a bank, i.e. administering the currency, and verifying and carrying out transactions.[455] The blockchain, however, records all transactions ever carried out on the system, including newly mined bitcoin. This is also the solution to the double-spending problem, mentioned at the beginning of this section. If a user transfers a bitcoin first to one user, and then tries to send the same bitcoin to another user in a second transaction, the first transaction will already be recorded in the blockchain, visible to anyone, with an exact timestamp that shows that that transaction was earlier. Other users and miners will verify the first transaction and reject the second, as at

452 Anderson (2014), p. 434.
453 If one bitcoin was traded for 1000 Euros, one Satoshi would be the equivalent of 0,001 cents.
454 Sorge/Krohn-Grimberghe (2012), p. 480 f.
455 Böhme et al. (2014), p. 2; Raman (2013), p. 68; Hildner (2016), p. 487. See for technical details concerning the cryptography Tschorsch/Scheuermann (2016), p. 2087 ff.

the point in time when the second transaction should have taken place, the bitcoin were no longer in the possession of the sender. *Nakamoto* himself explained it in these terms: "Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle."[456]

The transaction-based record of the blockchain is very different from the ordinary system employed by banks. This is explained very well by *Böhme et al.* with the following example of a series of transactions:

> "For instance, some user Charlie does not simply 'hold' three bitcoins. Rather, Charlie participates in a publicly-verifiable transaction showing that he received three bitcoins from Bob. Charlie was able to verify that Bob could make that payment because there was a prior transaction in which Bob received three bitcoins from Alice. Indeed, each bitcoin can readily be traced back through all transactions in which it was used, and thus to the start of its circulation. A consequence of decentralized verification and consensus is that all transactions are readable by everyone in records stored in a widely replicated data structure. In general, transactions are ordered recursively by having the input of a transaction (roughly, the source of funds) refer to the output of a previous transaction (e.g. Bob pays Charlie using Bitcoin he received from Alice)."[457]

With every new block added to the system, new bitcoin are added and brought into circulation. With an account of all newly added units and all transactions ever carried out in the system, any user's computer system can calculate and account for each unit at any time. No central authority is thus needed to clear transactions between users, as each user can verify any other user's possession of bitcoin by examining the blockchain.

This lack of a central authority is a primary and novel design feature of the bitcoin system, which, in the first place, secures transactions on the system. Secondly,

456 Nakamoto, cited in the p2pfoundation, no date.
457 Böhme et al. (2014), p. 2 f. See also Boehm/Pesch (2014), p. 76; Tschorsch/Scheuermann (2016), p. 2085 f.; Möser/Böhme/Breuker (2013), p. 3.

besides security and the removal of the double-spending problem, there is a further ideological component in the background. *Satoshi Nakamoto* himself gave this oft-quoted explanation:

> "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."[458]



One of the motivations is thus to do away with the powerful central structure of the banking system.[459] However, as *Weber* points out, while *Nakamoto* wished to do away with the necessity to trust in banks and to allow users more independence and self-governance, users of the Bitcoin system have to trust the technical architecture of the system in much the same way.[460] Indeed, most users of the Bitcoin system must trust the system as blindly as they must trust banks, as a large number of users will not have the technical expertise to comprehend the inner workings of the Bitcoin system. In addition, users have had to cope with a string of security breaches, data leaks and insolvencies of the major exchanges, on which most users depend to access and exit the Bitcoin economy.

The development of Bitcoin and *Satoshi Nakamoto's* explanation as cited above, should be seen in the historical and social context. Much of the critique of banks voiced in the community is certainly too broad, and may picture banks as more powerful entities than they really are.[461] However, Bitcoin was launched at the height of the financial crisis 2008, in which context much of the critique may have been justified if one-sided.

458 *Nakamoto*, cited in the p2pfoundation, no date. See also Bonaiuti (2016), p. 35 f.
459 Allaire (2013), p. 115 f.; Bonaiuti (2016), p. 35 f.
460 Weber (2013), p. 1.
461 Weber (2013), p. 3.

**iv. Miners and Cryptography**

Besides users, the system also requires miners. Miners basically use their computing power to keep the system running, and are rewarded with newly minted bitcoin in consideration. Every few minutes, a new set of transactions (a *block*) is added to the blockchain, containing all transactions that have taken place since the last block was added. This adds all new transactions to the ledger to store them in the history of Bitcoin transactions. A block is added by the miner who solves a pre-set cryptological problem the fastest.[462] The miners' computers must find an alphanumerical combination in order to 'win' the block, and that faster than all the others. The combination can only be guessed, by trying each combination until the correct one is found, in the same way as a *brute force attack* guesses a password.

The problems are designed in such a way that the solution is impossible to work out from the question, but that the answer can easily be verified once the solution is found.[463] A fitting analogy can be struck with a digit combination lock: the combination is impossible to infer from the exterior of the lock, so that in order to open it, one is forced to try every possible combination until one happens on the correct one and the lock opens. Also, the problems increase in difficulty as the miners' systems increase in computing power, in order to keep the rate at which blocks are added steady.[464]

The miner whose system guesses the answer to the problem first is rewarded with a fixed amount of bitcoin. In 2009 at the time when the genesis block was mined, a miner was rewarded with 50 bitcoin for each block. This number halves every 210,000 blocks. It has halved twice in the past; since July 2016, miners are rewarded with 12.5 bitcoin for each block. This way, eventually no new bitcoin will be added to the system and the number of bitcoin in existence will be fixed at about 21 million. Furthermore, miners are paid for keeping the system running through transaction fees that can be imposed on users.[465] Both the newly mined bitcoin and the transaction fees are meant as incentive for miners to continue participating and keeping the system running. This incentive appears to appeal to a large group

462 Murck (2013), p. 92; Stommel (2017), p. 8.
463 Böhme et al. (2014), p. 3; Holznagel/Tabbara (1998), p. 390; Tschorsch/Scheuermann (2016), p. 2086.
464 A new block is added on average every 5-10 minutes, see https://blockchain.info/ (last accessed 3 January, 2018). See also Murck (2013), p. 92; Holznagel/Tabbara (1998), p. 390.
465 Sorge/Krohn-Grimberghe (2012), p. 482.

of people, considering the vast amounts of computing power used to keep the system running and to mine bitcoin.

The central feature of this type of decentral virtual currencies thus lies in the use of cryptography to support the technical infrastructure. Cryptography is known to most people as a method of securing information from being accessed, altered, or stolen.[466] In virtual currencies, cryptography is used in that way, too, as the public key infrastructure allows users secure access to their accounts, or wallets.[467] But there is another feature to the system in which cryptography is used, which is to operate the blockchain.[468] The miners involved in maintaining the infrastructure must be involved in solving the puzzle set by the system in order to be able to add new blocks to the blockchain. It has been suggested that if a miner or a group of miners would reach a volume of computing power as to account for 51% of the combined computing power of all miners participating, this individual or group would be able to change the system and manipulate the blockchain at will (a *51%-attack*).[469] The system always accepts the longest blockchain as the most recent and therefore most accurate chain. Theoretically, someone could slip a manipulated transaction into a new block, but that block would have to be mined according to the rules of the system. This means that an attacker would have to mine and manipulate blocks faster than all other miners, for which command over 51% of the combined computing power of all miners would be necessary. However, considering how powerful the mining rigs are becoming,[470] such an attack is so unlikely as to be deemed impossible.[471]



**v. Third Party Services in the Virtual Currency Environment**

Finally, there are several businesses plugging into the virtual currency environment in order to facilitate its use.[472] There are three features that require some closer explanation and scrutiny, which are virtual currency exchanges, digital wallet services, and mixers.

466 Nicoll (2003), p. 109 f.; Stommel (2017), p. 10.
467 Böhme et al. (2014), p. 3; Raman (2013), p. 68.
468 Böhme et al. (2014), p. 3.
469 Anderson (2014), p. 434; Kasiyanto (2016), p. 154.
470 The network total amounted to 7983.858 Phash/s on January 3rd, 2018. Numbers available at https://bitcoincharts.com, last accessed 3 January, 2018. In comparison, the world's currently fastest supercomputer *Sunway TaihuLight* reaches a velocity of 93 Phash/s.
471 Böhme et al. (2014), p. 3.
472 Bonaiuti (2016), p. 41 f.; Hildner (2016), p. 488.

A virtual currency exchange is basically an online market place, where users can exchange virtual currencies for fiat currency.[473] Online exchanges work in much the same way as financial markets, but are limited in scope to virtual currencies. Most exchanges are operated in the form of a platform which brings sellers and buyers of one or more virtual currencies together, and charge a commission fee, usually below 2% of the value of the transaction.[474] Some exchanges also offer more sophisticated market tools, following the example of traditional stock exchange operations. Exchanges are to some degree gatekeepers for the virtual currency environment, as they are the main entry- and exit points for any user,[475] creating an interface between virtual currencies and fiat currencies. This function cements their immense importance to the virtual currency environment, but also makes them constant targets for attacks.

A great number of those exchanges have started up with the rise of virtual currencies worldwide, but the market is dominated by only 9 major players, who together served far over 90% of the market in the second half of 2016.[476] Those nine players are strewn all over the world. Four of the businesses are incorporated in the United States,[477] two are located in the European Union[478] (in Luxembourg and in the United Kingdom),[479] and two are located in China.[480] The ninth big player is the almost mysterious BTC-e, about which very few facts are known. The official website contains no address and no information on which natural persons stand behind the business, though the terms of service contains a forum selection clause indicating Cyprus as the chosen jurisdiction, and refer to anti-money laundering measures.[481]

473 FATF virtual currencies (2014), p. 9. See also CJEU C-264/14 *Hedqvist* [2015], paragraphs 22 ff.

474 Böhme et al. (2014), p. 5.

475 Rückert (2016), p. 12 f.

476 Böhme et al. (2014), p. 6; continually updated figures for each exchange can be found at bitcoinity.org (last accessed 3 January, 2018), and bitcoincharts.com (last accessed 3 January, 2018). The figures available at both of these sources can vary, especially depending on the way in which the size of the exchange is calculated. The author has chosen to follow bitcoinity's calculation based on the books, rather than the calculation based on self-reported volume.

477 The four exchanges in question are *Coinbase, Gemini, itBit*, and *Kraken*, which together served almost 35% of the market over the course of October 2016 (bitcoinity.org). All four of them are incorporated and licensed in the United States. Note that the market changes rapidly.

478 At the time of writing, the United Kingdom is still a Member State of the European Union.

479 The company *Bitstamp* is based in Luxembourg, and the exchange *cex.io* is based in the United Kingdom. Together they served over 15% of the market over the course of October 2016 (bitcoinity.org). Both exchanges are properly incorporated and licensed under national law.

480 Those two companies are *Bitfinex* and *OKcoin*, which together served approximately 32% of the market in October 2016 (bitcoinity.org). The status of incorporation and licensing of those two players in China could not be verified.

481 The terms can be found at https://btc-e.com/page/1 (last accessed 3 January, 2018).

Besides these big players, there are several other online exchange services, and some fora exist on which buyers and sellers of virtual currencies can connect, and then meet in the real world in order to exchange virtual currency for cash.[482]

When a user has exchanged fiat currency for virtual currency, the virtual currency value is stored in his or her wallet. A wallet is essentially a simple computer programme that contains the user's bitcoin, and which can be stored either on the user's computer, smart phone, or devices such as thumb drives, or it can be kept for the user by an online service.[483] Storage of the wallet file is a sensitive issue, because bitcoin, just as cash, can be lost or stolen. In the case of virtual currencies, the units are lost if the user loses access to his wallet file, either because of technical problems with accessing the file, or because the user forgot the password. Units can also be stolen if a third person gains access to the wallet file of the user. The wallet file is usually encrypted and secured with a password, but can be compromised on a user's computer with relative ease if the computer is not sufficiently secured against outside attacks. There are commercial services offering to secure the user's wallet for them, but vulnerabilities have been found in many of the commercial systems as well. While in the conventional banking system, the service provider to a large extent facilitates the security of the system for the customer, users of virtual currencies must be aware of, gauge and protect themselves against risks. This is another reason why virtual currencies appeal more to users with a certain level of technical literacy and experience.



Finally, one service which should be mentioned in this context is that provided by mixers.[484] A mixer is a service which is used to hide a user's transaction history in the blockchain by mixing the user's transactions seemingly at random with other user's transactions.[485] The result is that the transaction of the user to the mixer is visible, and then the blockchain shows clear indicators that a mixing service was used, but the funds are mixed in such a way with the transactions of other users, that the origin and destination of units cannot easily be linked to one another anymore. There are many reasons for using such a service, hiding criminal

482 See for example this news story by the Dutch department of public prosecution, https://www.om.nl/onderwerpen/ondermijnende/verhalen/bitcoinonderzoek/ (last accessed 3 January, 2018).
483 Böhme et al. (2014), p. 6. See also COM (2016) 450, p. 12 f.
484 Oerlemans et al. (2016), p. 109.
485 Boehm/Pesch (2014), p. 76; Tschorsch/Scheuermann (2016), p. 2108.

transactions and simply enhancing user privacy on the blockchain being the two prevalent ones.[486]

**vi. Who uses Virtual Currencies?**

This rather detailed discussion of how virtual currencies work and how they can be used naturally begs the question who the users are. The group of users of virtual currency systems is certainly far from homogeneous, and compared to the group of people using the conventional banking sector and/or Hawala, the amount of users of a virtual currency system is very small.[487] Users all share some degree of affinity for technical services and new technical developments, while a large segment of the population outside of the Bitcoin community still appears to view virtual currencies with distrust.[488] Other than sharing this trait, the user group has very little in common.

The fact that virtual currencies are necessarily only based online makes them less accessible for users with a low level of digital literacy, or with limited access to the internet. Also, once virtual currency units are acquired, users with a lower degree of technical expertise also face the added disadvantage of being vulnerable to attacks, as they may encounter difficulties securing their wallet files on their own computers, or must use an online service that administers their wallet files for them, which can also be vulnerable to security breaches beyond the control of the user.

Most users of virtual currency systems use virtual currencies for a certain reason, expecting a certain benefit or advantage from using virtual currencies rather than the conventional banking sector.[489] There are several potential benefits to users of virtual currencies. Payments could be made more efficient and easier in an international context.[490] Traders would only need to know the exchange rate of their home currency into a virtual currency, rather than calculating exchange rates for each other national currency they may come into contact with. Furthermore, transactions can be processed for lower fees than credit card transactions, which also allows for micropayments, small sums to be moved at low costs. Lastly,

486 Böhme et al. (2014), p. 6; Möser/Böhme/Breuker (2013), p. 5. See in this context also Simitis (1998), p. 2478.
487 Murck (2013), p. 94 f.
488 Murck (2013), p. 98; Filippi (2014), p. 9. See also Scholz-Fröhling (2017), p. 133.
489 Murck (2013), p. 95; Allaire (2013), p. 115 f.
490 FATF virtual currencies (2014), p. 8 f.; Anderson (2014), p. 431 f.; Bonaiuti (2016), p. 42 f.

transactions using virtual currencies can be much faster than transactions using regular banking channels. The relative ease with which exchange rates can be calculated, as well as the speed and low cost of transactions may make Bitcoin an attractive tool for e-commerce.

The number of bitcoin that will ever come into existence is capped at 21 million units, and the target is expected to be achieved in the year 2140.[491] As of January 3rd, 2018 one bitcoin is exchanged for ca. EUR 12.930 or ca. USD 15.048. In total, there are about 16.5 million bitcoin in existence at the time of writing, valued at over EUR 210 billion in total.[492] This limit and the scarcity appeal to investors, who see Bitcoin as an attractive vehicle for investments. In their reckoning, the price of bitcoin is likely to rise over time, when the supply diminishes and demand rises. As there is no central bank that can apply an economic policy and artificial stability to the currency, the exchange rate is extremely volatile and prone to large fluctuation in short time. This makes the use of Bitcoin at once risky and attractive for investors, as the potential for both gains and losses is great.



Furthermore, it has already been mentioned that many proponents of virtual currencies view the prevalent banking system with distrust and wish to be independent from it.[493] The open structure and decentralization of Bitcoin appeals to this group of people.

Finally, there is the group of users interested in the enhanced privacy virtual currencies are capable of facilitating. There are two main reasons, the first being a legitimate interest in privacy as explained above, and the second is the wish to secretly move value which is in some way connected to a crime. Very early in the history of Bitcoin, the potential for facilitating criminal transactions was recognized and acted upon. In order to use the Bitcoin system, a user needs not necessarily reveal his or her identity. Accessing the system is a little harder as most users will depend on the services of exchanges, but there are certainly many ways for users to acquire bitcoin without using an exchange, or by using a small exchange which allows users to use its service without (full) identification of the user, or even by managing to trick an exchange into accepting an incorrect

491 FATF virtual currencies (2014), p. 6; Murck (2013), p. 92.
492 Statistics at http://bitcoincharts.com, last accessed 3 January, 2018.
493 Murck (2013), p. 95; Allaire (2013), p. 116; Bonaiuti (2016), p. 42 f.

identity. Those users may wish to use Bitcoin to access one of the many online platforms in the dark web, on which drugs, weapons, and other illegal material is sold in exchange for virtual currency.[494]

### vii. Implication of Virtual Currencies in Financial Crime

There are many different online platforms for the sale of illegal goods and services. The payment method of choice is generally one of the established virtual currencies, most often bitcoin.[495] In the words of *Raman*, "Criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception."[496] From a point of view of a criminal user, the advantage of virtual currencies over conventional payment methods is the decentral structure of virtual currencies, which preclude one powerful entity to scrutinize all transactions and to watch out for suspicious patterns and potentially criminal transactions.[497] Certainly the blockchain can be scrutinized by anyone, user and third party alike, but there is no central authority to hold the key to the identities of all parties.[498]

This decentral structure and the possibility to use virtual currencies without such a third party knowing all users' identities often leads to virtual currencies erroneously being called anonymous. In the words of *Patrick Murck*, "Though it has sometimes been portrayed as such in careless media stories, Bitcoin is not a magic cloaking device that allows criminal actors free reign."[499] Instead, most virtual currencies should correctly be classified as pseudonymous[500] because although the user's names and addresses are not stored in the blockchain, the user's wallet address does appear in the blockchain. If the user takes no additional steps, his transaction record can be traced through the blockchain, linking him or her to other users, and potentially tracing the user to a seller or an exchange service in possession of his full identity.

Yet, finding a suspicious transaction, linking it to a user, and tracing that user's correct full identity[501] is naturally much more difficult on the blockchain than it is

494 Murck (2013), p. 98 f.; Boehm/Pesch (2014), p. 75.
495 Shasky Calvery (2013), p. 52 f.; Murck (2013), p. 98 f.; Boehm/Pesch (2014), p. 75.
496 Raman (2013), p. 67 f. See also Bonaiuti (2016), p. 45 f.
497 FATF virtual currencies (2014), p. 9; Raman (2013), p. 68.
498 Rückert (2016), p. 14 f.
499 Murck (2013), p. 96. See also Rückert (2016), p. 8; Möser/Böhme/Breuker (2013), p. 3.
500 Boehm/Pesch (2014), p. 75; Murck (2013), p. 96.
501 See also Article 29 Working Party Opinion 05/2014, p. 11; Allen (2013), p. 84.

for the conventional banking sector, where the identities of the parties are known to the central authority.[502] However, uncovering a user's identity is by no means impossible on a virtual currency platform. Few users of the Bitcoin system are likely to be versed enough in cryptography to hide their identities effectively and securely for a long time.[503] The open architecture of the system is treacherous in this regard. The blockchain will continue to be accessible to anyone for the foreseeable future, including to law enforcement agencies. Users wishing to conceal their identities must therefore be aware that traces of their transactions will be visible for several years after the transaction.



## e. Informal Value Transfer Systems

A second system for financial transfers existing outside and alongside the traditional banking sector is the Hawala system. In this context, Hawala will stand exemplary for the large amount of other informal value transfer systems, sometimes also called 'alternative remittance systems', as it is the most commonly known and one of the most extensively used systems.

### i. Remittances

Informal value transfer systems are predominantly and widely used by the immigrant communities living in Europe in order to send remittances back to their home communities and families. Remittances can broadly be defined as "funds received from migrants working abroad".[504] The amount of funds sent and received worldwide as remittances is difficult to estimate and figures can vary considerably, but the volume is generally believed to be significant and increasing. *Aggarwal, Demirgüc-Kunt and Peria* estimate the volume of remittances from industrial countries to developing countries at about 90 billion US dollar in 2003.[505] With this volume, workers' remittances are now an increasingly important source of external revenue, second only to foreign direct investment.[506]

502 Naturally, it is possible to hide one's identity also on the conventional banking system, for instance by using alternative identity documents or by using a sophisticated scheme of shell companies and trusts. See also Chapter II above.
503 Allen (2013), p. 84; Möser/Böhme/Breuker (2013), p. 3.
504 Aggarwal/Demirgüc-Kunt/Peria (2006), p. 1.
505 Aggarwal/Demirgüc-Kunt/Peria (2006), p. 1.
506 Aggarwal/Demirgüc-Kunt/Peria (2006), p. 1.

Remittances can flow through formal and informal channels. Formal channels for transferring remittances include banks as well as transfer services such as *WesternUnion* and *MoneyGram*.[507] Informal channels include alternative remittance systems, which are not licensed and often operate underground. The word 'alternative' should thus be understood as meaning an alternative to the formal banking system in the country from which the remittances are sent.

*Freund and Spatafora* define alternative remittances as "all types of money transfer services that do not involve formal contracts, and hence are unlikely to be recorded in national accounts."[508] Examples of such informal channels are for instance "cash transfers based on personal relationships through business people, or carried out by courier companies, friends, relatives or oneself."[509] One of the most prevalent networks for such informal cash transfer is Hawala, but a large number of similar systems can be identified, each operating under a different name, including the Filipino network of 'Padala',[510] the 'Hundi' system most prevalent in India,[511] a system known as 'Hui Kuan' in Hong Kong,[512] 'Phei Kwan' used in Thailand,[513] and finally the infamous 'Black Market Peso Exchange' active between North and South America.[514]

**ii. History and Development**

Hawala is a very old system for transferring money, and one of the most important channels of underground banking as well as a major alternative remittance system.[515] The system is prevalent in the Near and Middle East, and one of the most important transfer systems for countries such as India, Afghanistan, and Pakistan.[516] Literally translated from Arabic, Hawala means 'transfer'.[517] Persons acting as agents or nodes in the system are called *hawaladars*.

507 Freund/Spatafora (2005), p. 2. See also Reimer/Wilhelm (2008), p. 235.
508 Freund/Spatafora (2005), p. 2.
509 Freund/Spatafora (2005), p. 2.
510 Razavi (2005), p. 280; Passas (2006), p. 48.
511 Razavi (2005), p. 280; Passas (2006), p. 48. See also Sharma (2006), p. 105 and Marin (2009), p. 910 f. for an account of the differences between Hundi and Hawala.
512 Razavi (2005), p. 281.
513 Razavi (2005), p. 281.
514 Razavi (2005), p. 281.
515 FATF Hawala (2013), p. 9.
516 Sorel (2003), p. 376; Ryder (2007), p. 826; Schramm/Taube (2003), p. 407.
517 See also Passas (2006), p. 49; Marin (2009), p. 911.

The historical development of Hawala as well as that of most, if not all other informal transfer systems, are shrouded in mystery. It is impossible to give a precise timeframe or a narrow geographical area with which to credit the development of Hawala. The details of how the financial system has evolved are still disputed. Some accounts trace financial transfer systems like Hawala back to 5800 BC.[518] The history of these systems is often linked to the history of the Silk Road and the interests of travelling merchants along this route. It is supposed that the risk of robberies made it too dangerous for these merchants to carry the proceeds of their trade along with them on their travels, for which reason they preferred to use the services of a financial transfer agent in order to transfer their funds.[519] However, whether these are truly the roots of the system, or if the travelling merchants along the Silk Road were just one of many distinct groups of customers of a system much more ancient than that, cannot be said with certainty.

Hawala in particular shares its development in the Middle Ages with other similar systems prevalent in Asia. Hawala offered a means to send funds to a recipient some distance away, thereby facilitating commerce.[520] As *Razavi* explains,

> "[e]xpansion in commerce and trade during the early Islamic period created the need for a more sophisticated monetary infrastructure. Although silver coinage was a recognized method of payment in many areas, industry growth proved the supply of coinage to be insufficient. […] Within this historical and cultural setting, a group of institutions slowly established themselves and operated under influence of Islamic banking practices, as outlined within the Koran (the holy book of Muslims), and the Sharia (the body of Islamic law). Over time, this method of remittance became known as Hawala."[521]

Therefore, it can be said that Hawala is extremely old, in any case older than Islam itself, but the importance it has in the world today is likely due to its coincidence in geographic location with the religious centres of Islam, and the fact that either the practice was already compliant with the religious rules, or else could easily be moulded into the shape prescribed by Islamic law.

518 Razavi (2005), p. 280.
519 Razavi (2005), p. 280; Schramm/Taube (2003), p. 406 f.
520 Razavi (2005), p. 281.
521 Razavi (2005), p. 280 f.

### iii. Definitions

The great diversity of systems and traditions that can all be collected under the term informal value transfer systems makes the definition of this term difficult. The Financial Action Task Force uses the term 'Hawala and other similar service providers' (abbreviated as HOSSPs), and gives the following definition for this term:

> "HOSSPs, for the purpose of this typology, are defined as money transmitters, particularly with ties to specific geography regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash and net settlement over a long period of time. Some HOSSPs have ties to particular geographic regions and are described using a variety of specific terms, including Hawala, Hundi, and underground banking. While they often use banking channels to settle between receiving and pay-out agents, what makes them distinct from other money transmitters is their use of non-bank settlement methods, including settlement via trade and cash, as well as prolonged settlement time. There is also a general agreement as to what they are not: global money transfer networks (including agents) operated by large multinational money transmitters and money transfers carried out through new payment methods including mobile money remittance services."[522]

This definition already shows the difficulty in defining the concept of informal value transfer systems.[523] The 'Western' ideas of banking are almost incompatible with the practice of Hawala, as the two systems operate in entirely different ways. The conventional banking system and its organisation is so entrenched in the European culture that many regulators can hardly imagine that alternatives to it could exist at all. At the same time, the Hawala system is equally entrenched in the cultures in which it in turn is prevalent.[524] This difficulty is nicely illustrated by an anecdote shared about the British occupation of the Indian subcontinent.

> "The British had no real depth of understanding in relation to indigenous institutions, and there was a keen consciousness of this in some quarters.

522 FATF Hawala (2013), p. 9.
523 Marin (2009), p. 909.
524 Ryder (2007), p. 828 f.; Schramm/Taube (2003), p. 416.

> When the government enquired of select officials whether the terms 'bills of exchange' and 'hundi' should be defined in the ISA [Indian Stamp Act] of 1879, one response indicated that an embarrassing ignorance of this area was more likely to be uncovered than any real benefit for the law: 'The Assistant Commissioner, Ajmere, thinks it undesirable to define the word 'hundi', as a complete definition of the word would, he conceives, be difficult to find and be more likely to embarrass than to assist Courts and Revenue officers."[525]



It will be seen that these difficulties still manifest themselves in 2017.[526]

A more attribute-based approach may be most useful in explaining what Hawala in fact is to anyone not previously acquainted with the concept. The FATF gives a very helpful summary of the attributes of Hawala networks. It lists seven attributes that hawaladars will generally share, so that it can be said that hawaladars usually

> "(a) Are cash-in and cash-out businesses that primarily send personal remittances of low value. This does not preclude them from sending high value business transfers.
>
> (b) Operate in areas with high percentages of expatriate workers (in particular in originating countries), often in competition with other money transmitters.
>
> (c) Offer legitimate financial services to migrants sending remittances; however, they can also be used (or abused) for illegitimate purposes to move illegal/illicit money across the borders.
>
> (d) Operate within a community, are visible and accessible to their customers, are able to know their customers and maintain accurate records sufficient to ensure they complete transactions whilst preserving their profit
>
> (e) Run other businesses in addition to money transfer

525 The Finance and Commerce Departement, April 1896, 1-2, quoted in Martin (2015), p. 71. See for a similar account Marin (2009), p. 914 f.
526 See for instance section (d) of Chapter IV below.

> (f) Belong to networks of similar operators in other countries.
>
> (g) Communicate only limited information on the customer and beneficiary as far as individual transactions are concerned. This communication is limited to what is needed to complete the transaction. This information generally includes the beneficiary name, contact number and may also include a transaction reference number (code number/words to identify recipients), in order to ensure that the delivery is made to the right person in an efficient manner."[527]

To sum up, informal transfer systems as meant in the context of this thesis are all Hawala networks, and networks operating in the same way as Hawala does, and which operate illegally or at least outside of the regulated banking sector.[528] Just as Bitcoin often stands as an example for all virtual currencies, Hawala will serve as an example for all informal transfer systems of its type.

**iv. How it Works**

Basically, Hawala is a network of hawaladars. Just like virtual currencies, Hawala is a decentral system: there is no central agency that oversees the transactions, nor is there much government oversight in most countries.

To explain it in simple terms, it is best to make use of an illustrative example.[529] Imagine a hawaladar A in Amsterdam, and another hawaladar B in Lahore. Now there is a big Pakistani expatriate community in the Netherlands, and the young worker Bilal is one of them. Bilal has a large family in the central districts of Lahore, and saves a part of his wage in order to send it to his family in Pakistan, thereby sharing in the medical and educational expenses of his siblings. Nobody in Bilal's family has a bank account, so Hawala is virtually the only option for Bilal when choosing a way to securely send his remittances. He thus visits hawaladar A in Amsterdam, who operates a little ethnic food store and provides Hawala services to people in his community whenever needed. Bilal gives hawaladar A three hundred euro in cash and asks him to send it to Lahore to be paid out to

527 FATF Hawala (2013), p. 13. See also Pieke/Van Hear/Lindley (2007), p. 359 for a critique of the general distinction between the conventional banking sector and informal value transfer systems.
528 See also Marin (2009), p. 929 f.
529 See also Wheatley (2005), p. 349 ff.

Bilal's family. Hawaladar A subsequently calls his contact, hawaladar B, and asks him to pay out the value of EUR 300 in rupees to Bilal's younger brother, who arrives the next day to pick up the money. The transaction is completed.

Special about Hawala is thus the informality of the transaction, and the fact that the cash physically never moved from hawaladar A in Amsterdam.[530] When hawaladar B paid out the equivalent of three hundred euro to Bilal's brother, hawaladar A became indebted to hawaladar B for this amount. This debt is settled in subsequent transactions, explained below in a second example.



Haroon is a well-to-do merchant, who lives with his family in Lahore. His daughter Sana goes to University in Amsterdam. In order to finance her studies, Haroon regularly sends her money for her rent and general living expenses through the formal banking sector. However, Sana had an accident recently, and has incurred costs of three hundred euros through this accident. Haroon sends her extra funds to cover her expenses, but doesn't trust the formal banking system to transfer the amount fast enough. He thus visits hawaladar B, pays him the amount of rupees corresponding to three hundred euros, and asks him to transfer the funds to Amsterdam quickly. Hawaladar B calls hawaladar A on the phone and asks him to pay three hundred euro out to Sana, who, alerted by a text message from her father, arrives only a few minutes later at the office of hawaladar A to pick up the money. The transaction is completed.

This second transaction then cancels out the debt between the hawaladars incurred in the first transaction and balances their books.

Of course, the two examples given above only serve to explain how Hawala works in general terms, and are oversimplified for this purpose. In real life, the system is not linear from A to B and back, but rather dendritic and intertwined, as each hawaladar does not only connect to one other hawaladar, but has a number of different contacts in different cities and regions. This makes balances more difficult to even out, and requires extensive bookkeeping. Methods that can be employed to restore balances of accounts are, among other strategies, to create cash pools between a number of hawaladars to decrease the number of actors, going through brokers, or to route transactions via a third hawaladar in order

530 See also Schramm/Taube (2003), p. 407 f.

to even out a balance with that hawaladar.[531] Otherwise, traditional methods of transferring excess cash from one hawaladar to another are used, such as regular bank transfers or bulk cash smuggling from one hawaladar to another, or, if there are business relations, goods and services may be over- or under invoiced in order to restore balance to the accounts.[532]

**v. Structure of the Network and Record Keeping**

Hawala is often described as one network, while in reality, the term Hawala really means the sum of several separate though interconnected networks. The different networks are often defined around the lines of nationality, ethnicity or language, and remittances flow for the most part from cities and countries to which a larger group of a certain population has migrated, to the native country or regions of these migrants.[533]

The inner workings of Hawala are very different from that of the formal banking system. There is no hierarchy in an organization which can best be described as an intricate "web of relationships", or network of networks.[534] Each hawaladar is basically a node in the system connecting to a number of other nodes with varying amounts of intensity, which in turn connect to further nodes. The network is kept stable by trust among the hawaladars, and by each individual hawaladar's interest in fostering a good reputation in order not to lose this trust.[535] In the words of *Calderon et al.*, "[t]he reputation of honest person actually permits an individual to credibly commit himself ex ante not to betray his partners ex post."[536] If a hawaladar conducts himself or his business in such a way as to damage his reputation, he is quick to lose the trust of his partners, and can thus be excluded from the network, thereby losing his business and often also his position in society.[537]

The social position of hawaladars in their communities is generally rather high. Naturally, a good reputation is indispensable to anyone who is entrusted

531 See also Razavy/Haggerty (2009), p. 140.
532 Redin/Calderón/Ferrero (2012), p. 16; the methods employed are similar to traditional methods of money laundering. As hawaladars operate illegally in many countries, the balancing of accounts needs to be undertaken covertly. See also European Commission (2004), p. 6; Passas (2003), p. 54.
533 See also Vlcek (2008), p. 287 f.
534 Redin/Calderón/Ferrero (2012), p. 13.
535 Redin/Calderón/Ferrero (2012), p. 13; Razavi (2005), p. 285.
536 Redin/Calderón/Ferrero (2012), p. 13; Schramm/Taube (2003), p. 415. See in this context also Simmel (1906), p. 453.
537 Redin/Calderón/Ferrero (2012), p. 13 f.

with financial services, especially in tight-knit communities.[538] The position of hawaladars is generally cemented and reinforced by this trust in their proper handling of the financial transactions for the communities. *Razavi* emphasizes also the family heritages sometimes involved in the business of a hawaladar.

> "Members within the same family regularly associate themselves with a particular dealer and over time a close bond forms between the dealer and his client to the point that the dealer becomes part of a larger extended family, together with bonds and alliances that are rarely broken or challenged. A particular family may deal with one Hawala dealer throughout generations."[539]



This high degree of trust in the hawaladar is at the same time a strong protection of the hawaladar's customers from fraud. If the hawaladar's entire family's reputation and social standing cements the trust of the community in the honesty of the hawaladar, the consequence of deceit would potentially be the loss of that social standing, and be felt by a large circle of persons.[540]

In the same way, the dealings among hawaladars themselves is equally supported by and based on the reputation and trust among the hawaladars. False steps can potentially be punished by the loss of trust of other hawaladars in the honesty of the offender, which would very quickly drive him out of business.[541] It is sometimes stated that the connections between hawaladars are so deeply rooted in trust that "unilateral payments are made without worrying about their security, and large amounts of money change hands with no formal bookkeeping".[542] This notion is likely very much exaggerated, however. The hawaladar's own interest in protecting his reputation makes it naturally necessary to avoid all mistakes, including inculpable oversights. While the degree of bookkeeping certainly is of a lower standard than in the formal banking sector, there certainly are records,[543] which furthermore are necessarily detailed and precise enough to satisfy the hawaladar of the absence of errors and mistakes.[544]

538 Razavi (2005), p. 285; Ercanbrack (2011), p. 72; Razavy/Haggerty (2009), p. 147.
539 Razavi (2005), p. 285. See also Pieke/Van Hear/Lindley (2007), p. 358.
540 Lascaux (2014), p. 89; FATF Hawala (2013), p. 20; Pieke/Van Hear/Lindley (2007), p. 358.
541 Razavi (2005), p. 286; Lascaux (2014), p. 89.
542 Lascaux (2014), p. 89.
543 See Soudijn (2015), p. 263; FATF Hawala (2013), p. 19; Passas (2006), p. 50 f.
544 FATF Hawala (2013), p. 19; Passas (2006), p. 50 f.

**vi. Statistics**

How much value is moved via Hawala annually is very uncertain, and difficult to guess, but authors are generally in agreement that the volume is high.[545] In some countries, such as India and Pakistan, Hawala is the most accessible and widespread vehicle for financial transfers, often event he only financial service available to the people.[546] In the words of *Houssein*, "Hawala serves more than half of the world, and far more than conventional banking, and serves it well."[547] It has been suggested that the Hawala network, and with it the volume of funds moved, has expanded significantly in recent decennia. The recent and ongoing waves of migration from the countries where Hawala is prevalent, has brought an increased demand of Hawala along with it, especially for the transfer of remittances.[548]

The conservative minimum estimate of annual Hawala transactions lies at around USD 200 billion, but the real extent of Hawala is almost certainly much larger.[549] According to a 2003 estimate, the Hawala network may transfer up to USD 2 trillion annually, accounting for ca. 2% of the total volume of international financial transactions.[550] An oft-cited local example for this large number is the fact that despite all efforts on the side of the regulators, the extent of the use of informal transfer systems in India is estimated to amount to no less than 40% of India's gross domestic product, possibly moving up to USD 680 billion.[551]

**vii. Who uses Hawala?**

The global trend of worker's migration made it necessary to develop a wide effective system for transferring remittances. Therefore, Hawala plays a major role in financial transfers from the European Union and North America to regions where Hawala is a culturally preferred method for financial transactions, as the cultural and economic ties between the expatriate population and their home countries make an efficient system for remittances necessary.[552] Apart from the cultural ties, Hawala is often the best option for the transfer of remittances for illegal foreign workers in developed countries, as their status as illegal immigrants

545 Redin/Calderón/Ferrero (2012), p. 3; Pieke/Van Hear/Lindley (2007), p. 351.
546 Ryder (2007), p. 826.
547 Houssein (2005), p. 88. See also Ryder (2007), p. 826.
548 Redin/Calderón/Ferrero (2012), p. 3 ff.; Pieke/Van Hear/Lindley (2007), p. 351; Vlcek (2008), p. 287 f.
549 Lascaux (2014), p. 94; Ryder (2007), p. 826.
550 Ryder (2007), p. 826.
551 Lascaux (2014), p. 94.
552 Houssein (2005), p. 88 f.; Passas (2006), p. 46 ff.

prevents them from accessing the formal banking sector for transactions. This group of people is often also hampered by a lack of formal papers, a language barrier, and sometimes illiteracy.

Hawala is of great regional importance in countries such as Afghanistan, Pakistan and India, and by no means only used for remittances.[553] Many people in this region of the world do not have access to bank accounts, which makes financial transfers exceedingly difficult.[554] Remote rural regions in these areas can often not be reached with banks, for several different reasons. First of all, a bank account can be costly, and poorer segments of the population of developing countries cannot spare the cost of maintaining a bank account, especially if they do not have a lot of money to store in such an account in the first place. Secondly, banks often do not have branches in remote regions, which physically distances people from banks. Lastly, regions of conflict have largely been abandoned by banks. Many areas in for example Somalia and Afghanistan can practically only be reached by Hawala, as no other channel for financial transfers extends to these regions.[555] The same applies in the case of embargoes: some countries cannot be reached by bank transfers because of an embargo being in place against financial transactions to that country, in which case many people will see Hawala as the best way to carry out financial transactions.



**viii. Advantages of Hawala**

One advantage of Hawala over a bank transfer is the speed of transactions. For example in the example given earlier, when hawaladar A receives money to be transacted, he can contact hawaladar B to complete the transaction almost right away. With modern methods of communication such as mobile phones and email, the transaction information will reach hawaladar B almost instantly, and the recipient of the money can collect his transfer within a very short time.[556] The time frame within which a transaction is completed is often much longer if undertaken

553 It is estimated that 50% of all financial transfers in India are carried out using informal channels. See FATF Typologies Report 2004/2005, p. 6 ff., 12. See also Ryder (2007), p. 826.

554 FATF Hawala (2013), p. 17 f., p 22.

555 FATF Hawala (2013), p. 18.

556 Razavi (2005), p. 280; Lascaux (2014), p. 93; FATF Hawala (2013), p. 17 – the time frame in which a transaction is usually completed is located between a "few hours or at the most one or two days". Redin/Calderón/Ferrero (2012), p. 10 estimate that "transactions are usually completed within 24 hours", with transactions between major cities being faster and between remoter rural areas being slower. Time difference naturally also plays a role in international transfers. See also Passas (2006), p. 50 f.; Pieke/Van Hear/Lindley (2007), p. 357.

through the formal banking network. The main reason for the higher speed of Hawala compared to banks is that hawaladars need not transfer the funds for each individual transaction, but rather fall back on net settlement.[557]

Furthermore, Hawala is very cost effective. hawaladars usually only charge a small fee for their service, on average 1-5% of the amount transferred,[558] which often amounts to circa 25-50% of the fee a bank would charge for the same transaction,[559] which makes remittances, especially from Europe and North America, a valuable source of income for families in developing countries. Other institutions such as *WesternUnion* and *MoneyGram*, who provide essentially the same service, often charge a much higher fee for transfers into certain areas.[560] The FATF identified the cost-effectiveness of Hawala as the main reason for the existence of the system in most jurisdictions.[561]

This cost-effectiveness is caused by several factors. In the first place, the overhead costs of most hawaladars in Europe are rather low, as they can often combine their Hawala business with another business, in many cases ethnic food stores as in our example above, or internet cafes and similar small businesses.[562] Furthermore, many hawaladars ask no fees at all for their services from members of their own communities.[563] Yet hawaladars can make a profit with their services, mainly because of the exchange rates:

> "The main source of profit for Hawaladars is the foreign exchange arbitrage between formal and parallel markets. Beyond local currencies, Hawaladars use hard currencies – mostly the US dollar – for their operations mainly because they do not fluctuate excessively in the short

557 FATF Hawala (2013), p. 17.
558 See Redin/Calderón/Ferrero (2012), p. 11 and Table 2.2 on p. 35 for details; Lascaux (2014), p. 93.
559 FATF Hawala (2013), p. 17; European Commission (2004), p. 7.
560 For example, the estimated fee for a transfer of 100 Euro by Western Union from the Netherlands to Afghanistan was 17% on June 23rd, 2014. See in this context also Reimer/Wilhelm (2008), p. 235.
561 FATF Hawala (2013), p. 17; Johnson (2011), p. 155; Pieke/Van Hear/Lindley (2007), p. 357.
562 Razavi (2005), p. 280; Raphaeli (2003), p. 70.
563 Razavi (2005), p. 280, quoting *Mohammed El-Qorchi*.

> run, they serve as a hedge against inflation and they are easily convertible to other currencies."[564]

A further advantage of Hawala in the eyes of its users is that Hawala caters to the cultural preferences of the user. Members of the immigrant communities often face barriers when attempting to access the formal banking system of the host country. Especially recent arrivals often lack the language skills necessary to manage their affairs with the formal banking sector, and especially among women, illiteracy is a common problem.[565] In this situation, many people will prefer turning back to Hawala, which is already familiar and administered by a member of the same expatriate community, who commands the trust of most, if not all other members of that community, rather than struggling with the formalistic and unfamiliar processes of the formal banking system.



It has already been mentioned that Hawala is the only reliable system for financial transactions in some areas of the world. The formal banking system remains in the early stages of development in many countries around the world. Especially people in rural or remote areas of developing countries Asia and Africa, and people in conflict areas have no access to any other provider of financial services other than through the local hawaladar.[566] An example that is named often in this connection is the fact that Hawala continued operations in the very turbulent 1990's in Somalia, while all formal banks discontinued operations and Hawala was thus the only avenue for financial transactions that remained available for the local population.[567]

**ix. Sharia Compliance**

In this context, it is important to note that many traditional Muslims consider banks incompatible with the rules of their faith, as charging fees for credit, a core business of banks, is specifically outlawed by the teachings of the Quran.[568] Indeed, the fact that Hawala as a system is sharia compliant is given as one of the most important reasons why practicing Members of the Muslim communities in Europe may choose Hawala over the other available financial transfer services.[569]

564 Redin/Calderón/Ferrero (2012), p. 16; Passas (2006), p. 56 f.
565 Redin/Calderón/Ferrero (2012), p. 12
566 Redin/Calderón/Ferrero (2012), p. 12; Ercanbrack (2011), p. 72; Pieke/Van Hear/Lindley (2007), p. 356.
567 Houssein (2005), p. 88 f.
568 Redin/Calderón/Ferrero (2012), p. 12; Ercanbrack (2011), p. 75 f.; Schramm/Taube (2003), p. 413; Thompson (2007), p. 296 f.
569 Johnson (2011), p. 156.

There are three main rules on financial dealings in the Sharia.[570] The first one is *Riba*, meaning to charge interest from lending, which is forbidden. Secondly, gambling or speculation with money is called *Maysir* and as such forbidden. The third rule is known as *Gharar* and means excessive uncertainty in financial dealings, which is also forbidden under Sharia law. In a related manner, all business activities must be *halal*, and none of the financial activities nor the parties with which business is being done should be involved in activities forbidden by Islamic law.

Hawala complies with the prohibition of *Riba, Gharar* and *Maysir*. The essential activity of a hawaladar is to transfer money, in which *Gharar* and *Maysir* generally are not involved. *Riba* is also not an issue in Hawala. Although hawaladars do charge a small sum for each financial transfer, this charge should not be seen as interest, but rather as a fee for the provision of services, which is certainly allowed under Islamic law.

Thus, based on the foregoing, it can be said that Hawala appeals to a large group of different people for a number of different reasons. The biggest group of users of the Hawala system in Europe today is made up of migrant workers who make a living abroad and send remittances to their country of origin to financially support their friends and family. But there are also other users of the system. Notably non-governmental organizations active in the aforementioned remote, rural, or conflict areas that can best be reached with Hawala, use this system to transfer funds to finance local aid or development projects.[571]

**x. Implication of Hawala in Terrorist Financing**

As has been shown in the previous sections, Hawala operations in Europe are most often used by migrants as a means to send remittances to their home countries. In fact, the group of legitimate users wishing to use Hawala in order to transfer remittances is the overwhelming majority among users of Hawala. But, as any system for financial transfers, Hawala is vulnerable to illegitimate uses.

In Europe, several interesting cases have been documented in which Hawala has been used for illegal transactions.[572] However, and interestingly, most of those cases

570 Redin/Calderón/Ferrero (2012), p. 10; Ercanbrack (2011), p. 72; Bälz (2002), p. 448.
571 Redin/Calderón/Ferrero (2012), p. 15; Ercanbrack (2011), p. 72.
572 Van de Bunt (2008), p. 694 ff.

centre around money laundering, rather than terrorist financing. Indeed, Hawala can, because of its unique structure, be used for a great many illegal activities, including terrorist financing and money laundering, but also for tax evasion and to circumvent embargoes and capital controls.[573] Yet, terrorist financing is the one illegal activity most often associated with Hawala by the public, presumably due to its prevalence in the Middle East.[574]



The Patriot Act,[575] adopted by the United States after the terrorist attacks of 2001, introduced stringent measures for oversight and traceability of financial transactions, including a rigorous know your customer (KYC)-regime to be observed by all financial institutions. The know your customer duties include the identification of users and the retention of the user's transaction history.[576] Money transmitters which are not attached to a bank became subject to strict licensing requirements,[577] which pushed many small money transmission services out of business, and led to a large number of hawaladars either going out of business or underground. The know your customer regime and licensing requirements found their way quickly via the FATF guidelines into national laws worldwide.[578]

Interestingly, the connection between Hawala and the specific terrorist attack of September 11th, 2001 are for the most part fictional. As *Redin, Calderón and Ferrero* put it,

> "In the aftermath of the terrorist attacks of September 11th, Hawala became related to terrorist financing. Although there was 'no evidence that the 9/11 conspirators employed Hawala as a means to move the money that funded the operation' (9/11 commission, 2004, p.499), the

573 Redin/Calderón/Ferrero (2012), p. 15; Ryder (2007), p. 827.
574 See FATF international best practices – combating the abuse of alternative remittance systems (2003), p. 5 ff.; Article 29 Working Party, Opinion 14/2011, p. 19. See also Ryder (2007), p. 825; Jamwal (2002), p. 181 ff.; Thompson (2007), p. 284.
575 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Pub. L. No. 107-56, 115 Stat. 272 (2001), codified as amended in different sections of 12, 15, 18, and 31 U.S.C.), commonly referred to as (USA) Patriot Act. See also Chapter II (d) above.
576 See *Gouvin* (2005), p. 977 f.
577 See FATF international best practices – combating the abuse of alternative remittance systems (2003), p. 3.
578 The FATF received a mandate to oversee measures against terrorism financing in October 2001.

> system became stereotyped as an illicit financial structure linked to Islamic fundamentalism and terrorism."[579]

In the same way, it has been said that terrorists prefer Hawala in order to conceal the flow of money in preparation of renewed attacks, as such transactions might raise red flags if carried out through the banking sector.[580] Based on the lack of knowledge of Hawala in the general public and in politicians, it is likely that Hawala was targeted as almost anything with a connection to the Middle East and Islam has been targeted in recent years based on an alleged connection to terrorism, while proof of such a connection is absent in most cases.

Hawala has thus been targeted very specifically since 2001 for the suspicion of large-scale abuse of the system for the purposes of terrorist financing. As has been seen, regulations have been put into place and updated in recent years to govern financial transactions, including Hawala. At the same time, the numbers of estimated volume of funds moved over the Hawala system cited earlier do not reflect any effect of the tightened regulation on the general popularity of Hawala.

**xi. Implication of Hawala in Money Laundering**

While the public attention is centred largely on the connection between Hawala and terrorist financing, the most interesting connection between Hawala and financial crime is the involvement of Hawala in large-scale money laundering operations.[581] All of the advantages enumerated earlier about Hawala benefit the migrant community when they wish to transfer remittances to other countries, but all of those features also make Hawala a highly interesting and desirable tool for criminal transactions.

Hawala is a tool perfectly suited for moving funds clandestinely. Moving money always involves a risk of detection, especially when smuggling bulk cash,[582] or when using the formal banking sector with its stronger oversight mechanisms. Hawala

579 Redin/Calderón/Ferrero (2012), p. 8. See also Ryder (2007), p. 825; Lambert (2002), p. 362; Razavy/Haggerty (2009), p. 152; Thompson (2007), p. 284 f.; Wheatley (2005), p. 358.

580 See the statement of Rep. *Evan Bayh* (d-IN) before the US Congress on November 14th, 2001 at http://www.gpo.gov/fdsys/pkg/CHRG-107shrg81714/html/CHRG-107shrg81714.htm (last accessed 3 January, 2018)

581 Lascaux (2014), p. 94; Johnson (2011), p. 157; Van de Bunt (2008), p. 694 ff.

582 See also FATF physical transportation of cash (2015), p. 27 ff.; European Commission (2004), p. 6; Passas (2003), p. 54 f.

offers a solution to this problem, by simply not physically moving the value at all, which avoids physical detection. Furthermore, the speed of transactions is a great advantage for criminal transactions.

Additionally, hawaladars often already operate underground, which makes their services potentially vulnerable to abuse for criminal transactions.[583] A hawaladar who needs to avoid the attention of the authorities because he operates a financial services business without a license is unlikely to inform the authorities of a suspicious transaction attempted or already carried out through his unlicensed business. Many hawaladars will simply prefer not to ask questions,[584] especially as large transactions naturally generate large revenue in fees and even more so in foreign exchange arbitrage if different currencies are involved.[585]



**xii. Resistance to Regulation**

Finally and connected to the previous sections, a major criticism of the Hawala network is its perceived secrecy and its resistance to official regulation. As has been mentioned before, most hawaladars operate underground.[586] Their services are generally used by a small community of immigrants from a certain country or region for remittances, and not by the general public, which is most often wholly unaware of the existence of the Hawala network.[587] Therefore, the operations of a hawaladar are perhaps not so much clandestine as simply part of a parallel society.

The majority of hawaladars indeed do not adhere to the regulations applicable to them. Most are not licensed, do not follow the official standards of bookkeeping, and do not comply with anti-money laundering regulations. The main reason appears to be connected to the need to keep the overhead costs down, and to avoid the sometimes very costly process of becoming licensed as a financial services business.

The political response to the irregular oversight over Hawala is generally limited to two strategies: "either prohibit its operations altogether (with a predictable result of its deeper entrenchment in the underground economic segment) or heavily

583 Razavy/Haggerty (2009), p. 150.
584 Soudijn (2015), p .262.
585 Soudijn (2015), p. 262 f.
586 Lascaux (2014), p. 94; Razavy/Haggerty (2009), p. 150; Marin (2009), p. 929 ff.
587 Despite the fact that hawaladars sometimes advertise their services openly, see Ryder (2007), p. 827 f.; Passas (2006), p. 46.

regulate its activities (which seems problematic due to its obscure nature)."[588] Neither of those strategies are promising or desirable. "Efforts at regulation and/or delegitimation of the Hawala financial services at best result in creating a gray zone, where clients and dealers have to navigate the alternative ways to protect their interests in the absence of any working instruments of formal supervision and legal enforcement of financial obligations."[589]

However, it is certainly incorrect and rather unfair to say that no hawaladar complies with the regulations applicable to him. While many hawaladars, especially those serving only a very small community, certainly have an interest in remaining unencumbered by regulations, there are many larger hawaladars who do adhere to the legal obligations.[590] Based on the foregoing, the main obligation in the focus of the public are the hawaladar's obligations to prevent the abuse of the services offered by him for criminal purposes. While a hawaladar certainly will not have the option to build an automated control system and invest much time in compliance, small victories are easily achieved. For instance, *Houssein* relates the example of a Somali Hawala company which introduced an automated data system, which allows easier access and reference to all data as well as a warning system flagging illegal transactions and even automated forwarding to the Financial Intelligence Unit.[591]

## f. Conclusion

This chapter answered two preliminary research questions concerning alternative transactions systems, namely what they are and how they function. The purpose of this chapter was to give a short but comprehensive explanation of the financial transfer systems, which are to be examined in the following chapters. It is important to be familiar with the concepts of informal value transfer systems and virtual currencies in order to understand the later discussion of the application of the legal rules to those systems, as well as to the conventional banking system, for which the legal rules are primarily written.

588 Lascaux (2014), p. 94. See also Johnson (2011), p. 155 f.; Marin (2009), p. 929 ff.
589 Lascaux (2014), p. 94. See also Ryder (2007), p. 828 f.; Ercanbrack (2011), p. 73.
590 Houssein (2005), p. 89 f.
591 Houssein (2005), p. 89 f.

When comparing the different means of financial transactions mentioned in the previous sections, the contrasts become very noticeable. For instance, cash transactions are completely anonymous, and transactions using the conventional banking sector come with complete identification of the parties. Cash is an absolutely analogue means of transaction, while virtual currencies rely completely on the internet, and the conventional banking sector is in the process of becoming completely virtual as well. The conventional banking sector is the most widely used intermediary for financial transactions, but as it is almost impossible to estimate precisely how many people in Europe use Hawala and virtual currencies, it is difficult to gauge the market shares of those two systems.

The implication of each system in financial crime has only been outlined very roughly at this point. However, it is important to keep in mind that each of the systems also serve a very legitimate need and are primarily used for legitimate purposes, although the illegitimate transactions will be in focus in the following chapters. Particularly the coverage of these systems by the Anti-money laundering Directive will be discussed in detail in the following Chapter IV.

# Chapter IV

## Alternative Transaction Systems within the Anti-money laundering Framework

## Outline:

a. Introduction
b. Impact on the Conventional Banking Sector
    i. Compliance with Legal Obligations
    ii. Costs and Effectiveness
    iii. Cash Transactions
c. Impact on Virtual Currencies
    i. Money Laundering through Virtual Currencies
    ii. Lack of Regulatory Activity
    iii. Virtual Currencies as Property
    iv. Obliged Entities
    v. Obligations
    vi. The Proposed Fifth Anti-money Laundering Directive
d. Impact on Informal Value Transfer Systems
    i. Money Laundering though Hawala
    ii. Regulatory Challenge
    iii. Hawaladars as Obliged Entities
    iv. Obligations
e. Conclusion

## a. Introduction

The previous two chapters have introduced anti-money laundering measures and alternative transactions systems. This present chapter will bring the two together. The purpose of this chapter is to explain how the anti-money laundering rules are applied to the different transaction systems. In so explaining, the chapter will answer the sub-question to the main research question concerning the inclusion of alternative transactions systems into the anti-money laundering framework. It will in particular go into details of how service providers of the virtual currency environment and hawaladars can be classified as obliged entities, and what obligations they must comply with.



This chapter will begin with the conventional banking sector, for which the money laundering measures have originally been designed. Banks are the most important group of obliged entities, and the obligations of the anti-money laundering framework is primarily designed to fit them. Hawala is not mentioned explicitly in the Directive. Virtual currencies are also omitted from the text of the fourth Anti-money laundering Directive, although the upcoming fifth Anti-money laundering Directive contains small but explicit connections to the virtual currency environment. At the same time, the open definitions used in some provisions of the fourth Anti-money laundering Directive may allow for the application of the obligations also to providers of alternative transactions services. It should be noted that how those systems now fit into the existing legal framework is still highly contended, particularly what concerns virtual currencies.[592] "Happy the nation where the knowledge of the law is not a science", wrote *Cesare Beccaria* in 1764.[593] It will be seen in the discussion of the classification of virtual currencies and Hawala into the terms of the Anti-money laundering Directive that the criticism implied in his statement remains true until today. Neither virtual currencies, despite proposed amendments to the law, nor Hawala are easily subsumed under the terms of the Directive.

This chapter will show how hawaladars and service providers connected to the virtual currency systems can be classified as obliged entities under the existing

592 See COM (2016) 450, p. 22. The Commission is of the opinion that virtual currencies are not covered by the fourth Anti-money laundering Directive, while other authors are of the opinion that the Directive already covers virtual currencies. See Kaiser (2016a), p. 214 f.
593 Beccaria (1819), p. 54.

legal framework, and in a second step, how they comply with the obligations applying to them. In addition, it will outline the upcoming changes to the law brought about by the fifth Anti-money laundering Directive, although it should be emphasised that the Directive is still in the law-making process and that therefore, changes may yet occur.

The academic discourse of the inclusion of alternative transactions systems into the anti-money laundering framework is still in its infancy. A prosperous discussion of alternative transaction systems is hampered by the apparent unfamiliarity of many parties with these alternative systems and the way they work.[594] Therefore, the detailed discussion of alternative transaction systems in this chapter may prove valuable to the academic discourse. It will add a classification of alternative transaction systems in the terms of the Directive, trace the difficulties with this classification, and discuss the changes to the terms of the Directive which are expected to be brought about by the upcoming amendment to the Directive.

This chapter is connected to both of the previous chapters in that it builds upon the information there given, and it may lead to a deeper understanding of alternative transaction systems as well as granting some insights into potential problems and lacunae in the law. It is furthermore connected to the upcoming chapters in that it rounds off the introduction of both the anti-money laundering measures and alternative transaction systems. The classification of alternative transaction systems into the terms of the Anti-money laundering Directive provides a basis upon which some detailed aspects are going to be discussed at later points in this thesis. Particularly the fact that the Anti-money laundering can cover alternative transaction systems only with difficulties leads to the question whether alternative transaction systems may perhaps offer more privacy to users than the convernional banking system does. This question will be answered in Chapter IX (j), after different aspects of this question were discussed in the present chapter as well as in Chapters VI (e) and VII (e) below.

This chapter is organised in a very similar way as the previous chapter. In the first place, the impact of the anti-money laundering framework on the conventional

594 For instance, it will be pointed out several times throughout this thesis that virtual currencies are not anonymous, although this is often erroneously stated in literature. See prominently the European Commission's statements to this effect in COM (2016) 450, p. 22.

banking sector is to be outlined in section (b). This section is kept short as much of the impact of these measures has already been outlined incidentally in Chapter II. The focus lies on the impact of the anti-money laundering measures on virtual currencies (c), and on informal value transfer services (d).

## b. Impact on the Conventional Banking Sector

### i. Compliance with Legal Obligations

The anti-money laundering legislation has had an extraordinary impact on the conventional banking sector, and shaped it significantly. The rules were specifically written for that sector, and the sanctions are designed in such a way as to ensure compliance of that sector.[595]



The rules of the anti-money laundering framework are particularly designed to detect money laundering operations in the layering stage. The measure employed most often for that end is to move the funds to other accounts,[596] in order to place some distance between the funds and their origin. The anti-money laundering rules help the investigation of such schemes in several ways.

In the first place, the identification of all customers of a financial services provider helps following the trail and assessing the scheme in terms of persons involved. The fourth Anti-money laundering Directive added and strengthened further measures for those frequent cases in which shell companies are used in order to hide the identities of the beneficial owners of a company.[597] The Commission states very clearly that "[u]nderstanding the beneficial ownership of companies is at the heart of the risk mitigation of financial crime and of prevention strategies for regulated firms."[598] The identification obligations of service providers is meant to create a consistent paper trail for all transactions. In theory, therefore, "[i]f any portion of the laundering network is examined, the related paper trails could lead a diligent investigator directly to the source of the criminal proceeds and unravel the money laundering network."[599]

595 Gerlach (2017), p. 177 f.
596 Jost/Sandhu (2000), p. 12.
597 COM (2016) 450, p. 16.
598 COM (2016) 450, p. 16.
599 Jost/Sandhu (2000), p. 12. See also Reimer/Wilhelm (2008), p. 240.

Furthermore, the monitoring obligations can be most effectively carried out by the conventional banking sector, as the large service providers also have the technical infrastructure, and possibly most importantly sufficiently deep pockets, to monitor transactions efficiently. While there is naturally a great risk that suspicious transactions are missed in the sheer volume of transactions being carried out through those systems, the infrastructure in place makes credit institutions by far the most active obliged parties in sending suspicious activity reports.[600]

**ii. Costs and Effectiveness**

In addition to the points mentioned above, it should be stated that these anti-money laundering efforts are certainly not always viewed favourably.[601] *Sorel* comes to a sober judgment, "judging from what has already been realized about laundering, it seems that it will only ever be partially efficient."[602] In particular the cost-benefit calculation is considered unsatisfactory by many authors. *Redin, Calderon, and Ferrero* judge that

> "it is evident that the actions taken by countries to meet international standards and reporting requirements have created a huge burden, for low income countries without the appropriate capacity and resources in particular, and for the banking industry in general, while overall compliance with international standards is low".[603]

This burden is particularly created by the costs of keeping up a sophisticated monitoring and reporting system. Within a year after the introduction of the customer due diligence regime in the United States, the financial institutions in that country had spent more than USD 11 billion on compliance with the new regime.[604] The *British Bankers Association* has estimated that compliance costs incurred by banks in the United Kingdom lie at around GBP 250 million.[605] The costs incurred in developing countries may be even higher, and growing.

600 FIU Jahresbericht 2014, p. 19; Sorel (2003), p. 374; Favarel-Garrigues/Godefroy/Lascoumes (2011), p. 183.
601 Sorel (2003), p. 374. See also section (g) of Chapter II on the criticisms often levelled against the anti-money laundering approach.
602 Sorel (2003), p. 374.
603 Redin/Calderón/Ferrero (2012), p. 9. See also Lennon/Walker (2009), p. 41.
604 Ryder (2007), p. 836.
605 Ryder (2007), p. 847.

A recent study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs on the effectiveness of terrorist financing rules also came to the conclusion that this burden has a negative effect on the overall effectiveness of anti-money laundering rules.[606] According to this study, the cooperation between the competent authorities and the private sector is going anything but smoothly. "This finding is especially pertinent in the field of CFT, where the cooperation of financial institutions and other private actors is the key."[607] It was found "that banks become risk-averse due to the costly and burdensome risk assessment rules that they must comply with. This kind of 'de-risking' may result in ethnic profiling[608] and reluctance to operate in certain (particularly African) countries."[609]



Furthermore, the reporting duties, the costs involved, and the threat of high sanctions on obliged parties is exercising high pressure on obliged entities, to which they react by over-reporting suspicious activity, effectively burying the Financial Intelligence Units in paperwork.[610] The study uses an example from France to illustrate this tension, stating that "public-private partnership on terrorist financing in France has been characterised by mutual weariness.[611] For example, the staff members of Tracfin (the French FIU) were found to be weary of bankers, who they perceived as simply covering themselves rather than submitting a 'real report'."[612]

Similar studies have been conducted in other countries as well, with very similar outcomes. *Bures* notes that representatives of the British financial services sector

> "'clearly believe that the UK has approached a "tipping point" where past, current and future costs of such legislation are perceived to be greater than

606 Wensink et al. (2017), p. 151.
607 Wensink et al. (2017), p. 151; Warde (2007), p. 238. See also Frasher (2016), p. 47 f.
608 See also Bou-Habib (2008), p. 152. Footnote added by the author.
609 Wensink et al. (2017), p. 151. See also Article 29 Working Party, Opinion 14/2011, p. 19; Lennon/Walker (2009), p. 41; Maras (2012), p. 73; Favarel-Garrigues/Godefroy/Lascoumes (2011), p. 183 f.
610 Wensink et al. (2017), p. 15; Ryder (2007), p. 836 f.; Zentes/Wybitul (2011), p. 94. See also section (d) of Chapter II above.
611 See also Favarel-Garrigues/Godefroy/Lascoumes (2011), p. 186 f. Footnote added by the author.
612 Wensink et al. (2017), p. 151. The same study also notes that only the FIU speaks of a "partnership", not the obliged entities. See also Frasher (2016), p. 47 f.

> the benefits'. The survey also revealed that '[o]verall, UK-based companies comply with AMLR in order to avoid sanctions from the authorities, and not because they perceive AMLR as representing good business practice or as being effective at combating money laundering."[613]

Finally, an illustrative remark made by *Sorel* on the nature and entrenchment of money laundering may be repeated here:

> "Put simply, it is noticeable that the diversity of actors, intermediary protagonists, instruments and places make its comprehension a very delicate task. New restrictions are followed by new 'inventions' to escape from the original restriction. At the end of the chain, entire sectors of the economy (as in Russia), indeed entire countries, are pervaded by this type of 'dirty' money, in such a way that the equilibrium becomes precarious and, like 'floating capital', such money is said to be indispensable to the economy. The price of globalization is that even if a reaction to terrorism was to increase the measures against this tendency, this would not change the general trend towards a more and more fluid circulation of capital and financial products."[614]

The final judgment on the effectiveness of the anti-money laundering rules in the conventional banking sector is therefore simply that, despite having generated an immense and costly organisational machinery, it has not yet been shown that the desired effect has been achieved. Indeed, it is not unreasonable to doubt that such effect will ever be achieved.[615] Particularly in the fight against terrorism, it is important to come to realise that "more than just legislation" is required if the fight against terrorism and terrorist financing is ever to be successful.[616]

How these rules on money laundering have impacted alternative transfer systems will be examined in the following sections (c) and (d) in this chapter.

---

613 Bures (2015), p. 229. *Bures* also adds that a "survey among banks in Switzerland, Germany and Singapore found that 'the AML rules' implementation is highly burdensome and causes significant costs and efforts throughout the banks' and that 'the impact of money laundering prevention on the predicate offences is small'." See also Chapter IX below.

614 Sorel (2003), p. 377. See also Favarel-Garrigues/Godefroy/Lascoumes (2011), p. 184 ff.

615 Ryder (2007), p. 836 f.; Lennon/Walker (2009), p. 41.

616 Ryder (2007), p. 848.

### iii. Cash Transactions

In addition to the other difficulties encountered in the fight against money laundering and terrorist financing, the persistent anonymity of cash transactions should be mentioned again.[617] The conventional banking sector, while being closely connected to cash transaction in the sense that bank accounts and cash machines are essential services for the cash economy, does not monitor cash transactions. However, the Commission points out that cash payments are a major facilitator for terrorist financing operations.[618] Particularly "the use of high denomination notes, in particular the EUR 500 note, is a problem reported by law enforcement authorities. These notes are in high demand among criminal elements who engage in physical transportation of cash due to their high value and low volume."[619]



The anti-money laundering framework obliges traders in goods to carry out customer due diligence checks when a customer makes a cash payment of EUR 10 000 or more.[620] There are also already controls of cash flows over the borders of the European Union.[621] To this latter obligation, the Commission wishes to add stricter controls of cash shipped in post and parcel.[622] In addition, the Commission wishes that the competent authorities should be able "to act upon lower amounts of cash where there are suspicions of illegal activity."[623]

Transactions in cash as such are not regulated, although the Commission has sometimes said that it may look into a possibility to introduce an upper limit to payments in cash.[624] The considerable opposition to this proposition makes it unlikely that such a rule will be introduced in the near future, but it should not be considered to be an impossibility.

617 See in this context also section (c) of Chapter III above.
618 COM (2016) 50 final, p. 10. See in this context also Eichler/Weichert (2011), p. 201.
619 COM (2016) 50 final, p. 10.
620 Article 2 (1) (e) 4AMLD.
621 Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, OJ L 309, 25.11.2005, p. 9–12.
622 COM (2016) 50 final, p. 10.
623 COM (2016) 50 final, p. 10.
624 COM (2016) 50 final, p. 10.

## c. Impact on Virtual Currencies

The impact of anti-money laundering measures on virtual currencies is rather difficult to gauge. Virtual currencies have developed in the presence of a rather sophisticated anti-money laundering framework, but they have also put unique challenges to the framework. As has been shown earlier, the anti-money laundering framework is based on the application of a set of four rather elaborate obligation on all service providers in the financial sector as well as selected neighbouring sectors. One obvious challenge is therefore to bring providers of innovative services connected to the virtual currency environment under the umbrella of the Anti-money laundering Directive. This section will show that the subsumption of such service providers under the terms of the Directive is rather complicated, but certainly possible. An as yet unsolved problem in this regard is the fact that service providers may be established anywhere in the world, including in third countries with little anti-money laundering oversight. This rather fundamental problem of the limits of national jurisdiction in an online context falls outside the scope of this thesis, however, and was not placed in the centre of the present inquiry.

Another challenge which should be discussed concerns the direct connection between users. The virtual currency system may be used without accessing the services of any obliged entity: Service providers facilitate the use of virtual currencies, but are by no means necessary. Therefore, users may access and make use of virtual currencies without the intervention of a third party. The effectiveness of the anti-money laundering approach on virtual currencies may therefore be questioned. At present, transactions made on the virtual currency system as such fall outside of the scope of the Directive in the same way as cash transactions do.

This section is going to walk the reader through these issues one by one. This section begins with a short discussion of money laundering operations which may be carried out using virtual currency systems, and relate the initial lack of regulatory activity in the field. The following sub-sections classify virtual currency as property, which defines virtual currencies as falling into the scope of the Directive, and argue that certain service providers connected to the virtual currency environment may be subsumed under the groups of obliged entities and must therefore comply with their obligations under the Directive. Finally, this

section will discuss the proposed update to the Directive and the changes this update will bring about for virtual currencies.

**i. Money Laundering through Virtual Currencies**

The emergence of virtual currencies has created a new attractive potential tool for money launderers. Virtual currencies allow for swift application of the three stages of money laundering.

The first stage, placement, is likely the most difficult stage to accomplish if virtual currencies are to be used for money laundering purposes.[625] The fact that virtual currencies are solely accessible online creates a pivotal gatekeeper role for online currency exchanges, as most users will use their services when entering and exiting the system.[626] The exchanges being based online makes electronic bank transfers the most convenient means to accept fiat currencies in exchange for virtual currencies. As has been outlined in the previous Chapter III already, most large exchanges are properly licensed in the jurisdiction in which they are established, and do comply with identification obligations as prescribed in the anti-money laundering legislation.[627] However, there are certainly also small exchanges which do not follow the anti-money laundering legislation and which do not identify and verify the identity of buyers.[628] Furthermore, while exchanges are the dominant entry and exit points to a virtual currency environment, they are not the only means to acquire units in virtual currency systems. There are several platforms online,[629] where potential buyers and sellers of virtual currency units can come into contact in order to allow them to exchange units among themselves without the intervention of a third party, such as an exchange.

Once the units have been acquired, the layering stage can be entered. The layering stage in virtual currencies is dominated by the fact that the blockchain records all activity carried out on the virtual currency system in the public ledger. The challenge of a money laundering operation using virtual currencies is thus to hide the layering activities in plain sight of anyone perusing the blockchain.[630]

625 See also Leslie (2014), p. 74.
626 Rückert (2016), p. 12 f. See also Oerlemans et al. (2016), p. 77.
627 See also CJEU C-264/14 *Hedqvist* [2015], paragraphs 22 ff. See also Shasky Calvery (2013), p. 57.
628 Rückert (2016), p. 11.
629 See for example this story published by the Dutch public prosecutor's office, https://www.om.nl/onderwerpen/ondermijnende/verhalen/bitcoinonderzoek/ (last accessed 3 January, 2018). See also Rückert (2016), p. 11.
630 Murck (2013), p. 100.

The layering stage is facilitated by the fact that wallets and bitcoin addresses can be created manually by the user without the intervention of a third party and therefore without the need to disclose one's identity to a business or service provider.[631] A money laundering operation may thus be accomplished by moving the units skilfully between different accounts held by the same person, making the movement appear legitimate, for example by allowing time to elapse and transferring small sums. Furthermore, there are the mixing services already mentioned in the previous chapter, which disconnect the addresses of origin and destination of funds in one transaction, by mixing the funds of that transaction with funds of other transactions, and moving units several times until the two parties to one transaction cannot easily be connected to one another, although it is by no means impossible.[632]

Finally, the integration stage has become very simple in larger and growing systems such as Bitcoin.[633] Keeping bitcoin as an investment, in order to speculate on a rise in value of the units, is an investment practiced in a small way by many people. Keeping bitcoin as an investment therefore would prima facie appear legitimate in itself. Furthermore, there are now many businesses accepting virtual currency units; virtual currencies are well on their way to being considered a mainstream financial channel. Both legitimate and illegitimate businesses use virtual currencies for payment.[634] The laundered virtual currency units may thus be used to buy legitimate goods and services, or they may be invested in further criminal activity on one of the illegitimate platforms.

Risk assessments carried out on the national level as well as by obliged entities will likely draw a very mixed picture of digital currencies. The novelty and short acquaintance of many regulators with virtual currencies, coupled with the notoriety of the various money laundering cases in which virtual currencies have been employed may potentially distort the view onto virtual currencies in some Member States, and cause them to classify virtual currencies in general as a high-risk vehicle.[635] Furthermore, it seems likely that the risk-based approach provided

631 Lowery (2013), p. 73.
632 Möser/Böhme/Breuker (2013), p. 5 f.
633 See also Leslie (2014), p. 75.
634 See in this context also Cannataci (2013), p. 10.
635 See in this context also Luther (2016), p. 401 f. for the initial negative reaction of American regulators to virtual currencies.

for in the fourth Anti-money laundering Directive will lead to fragmentation of the law, with different legal situations applying to virtual currencies in each Member State.

**ii. Lack of Regulatory Activity**

Policy-makers and law-makers have been experiencing difficulties with virtual currencies from the start.[636] In December 2013, the former President of the Dutch Central Bank, *Nout Wellink*, was quoted comparing Bitcoin with the Tulip Mania of the 17th century in the Netherlands.[637] This mind-set may explain the low speed with which virtual currencies have found their way on agendas of policy makers in Europe. However, it has been argued that virtual currencies, if left unregulated, could be a "powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities."[638] This perception has jolted the regulator into action.



Indeed, this quote illustrates the initial response by regulators to virtual currencies. The first reaction of most regulators was to try to ban or suppress virtual currencies as far as possible, as they were initially perceived primarily as a threat.[639] This was evident particularly in the United States, where it was openly demanded by members of the Senate that virtual currencies should be "shut down".[640] Such demands, however, are evidently based on a lack of understanding of the architecture of the system as well as of basic concepts of jurisdiction and the internet as such. It is not easily discernible how the government of any state should claim jurisdiction[641] over a global network of miners who themselves do not appear to be in violation of any existing statutes. Therefore, besides the occasional vociferous statements, the regulatory response has largely limited itself to issuing warnings against using virtual currencies.[642]

The third Anti-money laundering Directive 2005/60/EC was passed four years before the launch of the first successful virtual currency. The emergence of the

636 Giambelluca/Masi (2016), p. 15 f.
637 Hern (2013). See also Kütük/Sorge (2014), p. 643; Anderson (2014), p. 430; Filippi (2014), p. 4; Geva (2016), p. 285.
638 FATF Virtual Currencies (2014), p. 3. See also Luther (2016), p. 401 f.
639 Dowd (2014), p. 66 f.
640 Dowd (2014), p. 66. See also Luther (2016), p. 401 f.
641 Leslie (2014), p. 291 ff.
642 See for example European Banking Authority (2014), p. 23 ff.; Giambelluca/Masi (2016), p. 17 f.

new system was thus unforeseeable for the regulators at the time. The Directive reflected a reality in which few big players dominate the market for financial transactions. It placed emphasis on large established banks, credit card companies, and other transaction services to clear transactions and carry out customer due diligence checks on their customers.

The text of the fourth Anti-Money Laundering Directive also does not explicitly mention virtual currencies at all, not even in the recitals. The Commission did mention the "potential for misuse of new technologies to conceal transactions and hide identity"[643] when it first introduced the proposed text of the Directive, but did not elaborate on which technologies it refers to and how these new technologies should be brought under the umbrella of the proposed directive to mitigate the risks.[644]

However, in its most recent activity in the area of anti-money laundering and terrorist financing regulations, the legislator has begun to embrace an approach in which virtual currencies also play a role.[645] The Commission's Action Plan on the fight against terrorist financing, for instance, also mentions virtual currencies explicitly, stating that criminals, including terrorists, have not been slow to see the benefits of new technologies for their cause, and that virtual currencies may be abused for terrorist financing operations.[646]

> "New financial tools such as virtual currencies create new challenges in terms of combatting terrorist financing. Highly versatile criminals are quick to switch to new channels if existing ones become too risky. For innovative financial tools, it is critical to be able to manage the risk relating to their anonymity,[647] such as for virtual currencies."[648]

Seen in connection with the latest efforts of the Commission to bring forward a fifth Anti-money laundering Directive that would also cover virtual currencies, the era of regulatory inactivity may, therefore, now be declared to be ended.

643 COM(2013) 45 final, p. 4. See also Leith (2006), p. 115; Geva (2016), p. 285.
644 See also European Economic and Social Committee 13666/16, p. 4; Rückert (2016), p. 10.
645 See also FATF virtual currencies (2015), p. 14.
646 COM (2016) 50 final, p. 3.
647 *Sic*, see however the correct definition of anonymity in Chapter VII below. Footnote added by the author.
648 COM (2016) 50 final, p. 3. See also Anderson (2014), p. 432.

### iii. Virtual Currencies as Property

Virtual currencies can only fall into the scope of the Directive if they may be considered to fall under the definition of the term 'property' in article 3 (3) 4AMLD. It should be noted at the outset that the Commission is of the opinion that virtual currencies and providers of services related to the virtual currency environment are not regulated at EU level under the fourth Anti-money laundering Directive.[649] However, the open structure of the definitions used to define the scope of that Directive, one may find reasons to disagree.[650]

The lack of elaboration within the Directive on the question how virtual currencies are to be included in its scope, leads to much guesswork in whether and how virtual currencies should be covered. Yet, the Directive is drawn up in very broad terms, which facilitates the inclusion of virtual currencies. The Directive begins in article 1 (3) 4AMLD with the definition of money laundering, which includes

> "(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
>
> (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity;
>
> (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
>
> (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c)."

649 COM (2016) 50 final, p. 5; COM (2016) 450 final, p. 12.
650 See for more details Kaiser (2016a), p. 218 ff. See also Kütük/Sorge (2014), p. 645.

It will be noted that the definition of the term 'money laundering' does not speak of *money* specifically but rather more broadly of *property*.[651] The term 'property' is defined in article 3 (3) 4AMLD as meaning "assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets." Virtual currencies can therefore clearly fall into this definition.[652]

Besides money laundering, the Directive also covers terrorist financing. Terrorist financing is defined as "the provision or collection of funds, by any means, directly or indirectly, with the intention that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism." In contrast to money laundering, terrorist financing is thus concerned with 'funds' rather than 'property'. The Directive does not include a definition of the term 'funds', but the FATF guidelines included this term in the general glossary with a definition almost identical to the definition of 'property' in the Directive. The term 'funds' covers thus essentially the same items as the term 'property', and can therefore be considered to include virtual currencies as well.[653]

**iv. Obliged Entities**

If virtual currencies such as Bitcoin can thus be regarded as property within the meaning of the Directive, it follows that all services connected to the Bitcoin economy may be covered by the Directive as well. The term 'financial institution' is defined in article 3 (2) (a-f) of Directive 2015/849 as, primarily, "an undertaking other than a credit institution which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council, including the activities of currency exchange offices (bureaux de change)".[654]

The first and foremost obliged entity in the context of virtual currency systems is the online exchange service, in which users can exchange fiat currencies such as

651 See also section (b) of Chapter II above.
652 Beck (2015), p. 581.
653 See however Pesch/Böhme (2017), p. 95 about problems with the compatibility of virtual currencies and the German national anti-money laundering law.
654 Article 3 (2) (a) 4AMLD.

US dollar and Euros for virtual currencies.[655] Online exchange services may fall into the scope of the Directive as 'currency exchange office' within the meaning of article 3 (2) (a) of Directive 2015/849. The question whether virtual currency exchanges can be subsumed under the term 'currency exchange office' depends on whether or not the definition of a currency exchange office may be extended to cover virtual currency online exchanges by analogy.

However, most online exchange services work slightly differently than a classic currency exchange. The comparison to currency exchange offices may cover the activities of some exchanges, but others do not exchange themselves, but rather act as an intermediary between buyers and sellers in the way of a foreign exchange market. These exchanges bring buyers and sellers together in order to exchange virtual currencies, allow the laws of supply and demand to determine the exchange rate, and facilitate the exchange.



Again, the definition of financial institution in article 3 (2) (a) 4AMLD points to Annex I of directive 2013/36/EU of the European Parliament and of the Council. Point 7 of that Annex includes "7. Trading for own account or for account of customers in any of the following: (a) money market instruments (cheques, bills, certificates of deposit, etc.); (b) foreign exchange; (c) financial futures and options; (d) exchange and interest-rate instruments; (e) transferable securities." The foreign exchange market is therefore clearly covered.

The classification of the activities of online exchanges as either currency exchange offices or foreign exchange market places pivots on the classification of virtual currencies. Virtual currencies are generally not regarded as 'currencies'.[656] Although they have the three attributes commonly associated with money, which are that they serve as (1) a medium of exchange, (2) a unit of account and (3) a store of value,[657] they lack the essential element for currencies, which is that they are not issued by a country as the legal tender for that country; they are not to be considered as fiat currency.[658] The interpretative notes to the FATF Recommendations contain

655 Rückert (2016), p. 11.
656 Beck (2015), p. 580; FATF virtual currencies (2014), p. 4. See also ECB Opinion 13303/16, p. 3; Beck (2015), p. 580 f.; Bonaiuti (2016), p. 36.
657 See Chapter III above.
658 Engelhardt/Klein (2014), p. 356; Kubát (2015), p. 410 ff.; Sorge/Krohn-Grimberghe (2012), p. 484.

a general glossary of terms, which defines that "[c]urrency refers to banknotes and coins that are in circulations as a medium of exchange."[659] The reference to banknotes and coins is somewhat problematic for virtual currencies, which are marked by the distinctive feature of not having any official printed banknotes or minted coins, but it is equally problematic for fiat currency. It cannot be expected that the presence of tangible bills and coins constitutes a very important element of the definition, as the term should not only cover cash but rather also electronic money, which is of course of immense importance in financial transfers. Considering that the definition of the term currency is by no means cast in stone and predates the internet as we know it as well as the possibilities it opened for global virtual currency schemes, it may be argued that although virtual currencies are not currencies as such, virtual currencies can be equated with fiat currency for the purposes of anti-money laundering legislation.[660]

Therefore, service providers plugging into the Bitcoin economy, facilitating online exchange from fiat currency into bitcoin and vice versa, are financial institutions within the meaning of Directive 2015/849, either comparable to currency exchange offices or to foreign exchange marketplaces, depending on the internal organisation of the exchange. Exchanges must therefore comply with the obligations set forth in the Directive.

It should be pointed out that this opinion[661] is not shared by the European Commission. On the contrary, the Commission states that "Providers of exchange services between virtual currencies and fiat currencies (that is to say currencies declared to be legal tender) as well as custodian wallet providers for virtual currencies are under no obligation to identify suspicious activity."[662] This is one of the reasons why the Commission has become active and proposed an update to the framework with the fifth Anti-money laundering Directive.

In this context, it should also be noted that currency exchange offices of the analogue variety are considered to entail an increased money laundering risk due

659 FATF Recommendations 2013, p. 112; see also Anderson (2014), p. 428 f.; Kubát (2015), p. 411.
660 Kaiser (2016a), p. 214 f.
661 Kaiser (2016a), p. 214 f.; Shasky Calvery (2013), p. 57.
662 COM (2016) 450, p. 22.

to difficulties in oversight.[663] It is too early yet to say how well online exchange services will cope with their anti-money laundering obligations, but it is likely that similar difficulties as with their offline counterparts will present themselves.

**v. Obligations**

The obligations with which obliged parties must comply then also apply to services plugging into the virtual currency environment. However, the nature of virtual currencies makes the full application of the anti-money laundering framework very difficult.[664]



Naturally, each obliged entity must comply with the identification requirements set out in the Directive. In particular the identification requirements are to be complied with. Service providers therefore must take steps to establish and verify the identities of customers in a way that is convenient for both the businesses and the customer, which is made a little more difficult by the fact that most service providers operating with virtual currencies necessarily operate online. Identification of users of virtual currencies can be accomplished in several different ways. For instance, some service providers for instance require that an account on their platform is linked to a bank account held at a conventional bank.[665] In other cases, electronic identification options can be explored by obliged entities in order to comply with their obligation.[666]

Difficulties arise in connection with the monitoring and reporting obligations. Obliged entities in the virtual currency environment are only charged with the obligations matching the services they provide. Most of the obliged entities providing services in the virtual currency cannot be charged with extensive monitoring obligations, as the vast majority of transactions take place on the system, outside of the area of their influence.[667] The Commission recognises this problem. It states that

> "The inclusion of virtual exchange platforms and custodian wallet providers will not entirely address the issue of anonymity attached

663 Sorel (2003), p. 376.
664 FATF virtual currencies (2015), p. 14 ff.
665 Hendrickson/Hogan/Luther (2014), p. 5.
666 COM (2016) 450, p. 19.
667 Raman (2013), p. 68; Möser/Böhme/Breuker (2013), p. 1.

> to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without exchange platforms or custodian wallet providers."[668]

Whether this problem can be solved effectively by regulation is not clear.

The reporting obligations also affect providers of services in the virtual currency environment. However, the limited scope of monitoring limits the possible moments of suspicion to a large extent, and will therefore likely not be extremely effective. In the conventional banking sector, the overwhelming majority of suspicious transactions reports are made by banks, and only very few are made by financial institutions such as currency exchange offices.[669] It is likely that service providers connecting to virtual currencies would develop similarly.

Finally, it should be pointed out that a parallel to cash transactions could be explored in this context.[670] As the virtual currency environment is very similar to cash in the regard that transactions between users on the system are not monitored, a remaining possibility would be to apply the rules concerning cash transactions also to virtual currencies. This would entail a lack of monitoring of direct transactions between users, but also extending the obligations of traders in high-value goods to transactions in virtual currencies. Pursuant to article 11 (c) 4AMLD, whenever a seller of goods carries out a transaction valued at EUR 10 000 or more, the seller is under an obligation to carry out customer due diligence measures.[671] Naturally, the equivalent of EUR 10 000 in another currency should also be covered by the same rules, and transactions in virtual currency may therefore be treated in the same way whenever the value of the transaction is the equivalent of that amount. Such an option has not, however, been explored by the lawmaker so far.

**vi. The Proposed Fifth Anti-Money Laundering Directive**

As has been mentioned before, the fourth Anti-money laundering Directive was passed in May 2015, at a point when virtual currencies were already receiving a high level of attention, and gaining in value and expanding their user bases rapidly. Passing the new Directive without so much as a reference to virtual

668 COM (2016) 450, p. 22.
669 See for instance FIU Jahresbericht 2016, p. 10.
670 Kaiser (2016b), p. 32.
671 See also Chapter II section (e) above.

currencies thus seems a rare omission, and a lost chance to create legal certainty.[672] In the words of the Director of the United States Financial Crimes Enforcement Network FinCEN, "We understood that AML protections must keep pace with the emergence of new payment systems, such as virtual currency and prepaid cards, lest those innovations become a favoured tool of illicit actors."[673]

This opinion seems to have been shared by some voices within the European Commission. In July 2016, the Commission thus created the strange situation in which the third Anti-money laundering Directive was in effect, the fourth Anti-money laundering Directive was passed and due to enter into force in June 2017, and a fifth Anti-money laundering Directive was already proposed.[674] The proposal of the fifth Anti-money laundering Directive is particularly interesting in this context because it seeks to remedy the deficiency of the previous framework regarding the omission of virtual currencies. The lacuna in the law of a lack of regulatory oversight over virtual currencies is one of the main concerns identified by the Commission, prompting it to act.[675] The amendment is the introduction of a three-level structure,

> "(i) bringing virtual currency exchange platforms and (ii) custodial wallet providers under the scope of the Directive, while (iii) allowing more time to consider options as regards a system of voluntary self-identification of virtual currency users."[676]

Of particular interest are the two recitals to the proposed fifth Anti-money laundering Directive discussing virtual currencies. Recital 6 5AMLD addresses the fact that transactions between users on the virtual currency environment are not monitored by any obliged entity. The Commission therefore reasons that instead of obliged entities, "[c]ompetent authorities should be able to monitor the use of virtual currencies. This would provide a balanced and proportional approach,

672 See in this context also Bieker/Hansen (2017), p. 286 f.
673 Shasky Calvery (2013), p. 55. See also Giambelluca/Masi (2016), p. 16 f.
674 COM (2016) 450: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 Directive 2009/101/EC.
675 COM (2016) 450, p. 9.
676 COM (2016) 450, p. 9. See also Hildner (2016), p. 492 f.

safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship."[677]

How this monitoring should be achieved is further elaborated in the following recital 7 5AMLD in the version of its original proposal by the Commission. The Commission stated that "The credibility of virtual currencies will not rise if they are used for criminal purposes. In this context, anonymity[678] will become more a hindrance than an asset for virtual currencies taking up and their potential benefits to spread."[679] The Commission states this sentiment as follows:

> "The anonymity of virtual currencies allows their potential misuse for criminal purposes. The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without these providers. To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to obtain information allowing to associate virtual currency addresses to the identity of the owner of virtual currencies. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed."[680]

The Commission is therefore convinced that virtual currencies cannot continue to exist in the way they have until now. The latest sharp increase in price per unit[681] appears to contradict this statement, however.

The amendments to the substantive articles of the Directive reflect the visions outlined in the recitals only to a certain degree. Article 2 (3) of the Anti-money

677 COM (2016) 450, p. 22. See also Shasky Calvery (2013), p. 57.
678 Note that the term 'anonymity' is here incorrectly applied. The fifth compromise text changes the wording of the recital slightly, but still uses the term 'anonymity'. For a more detailed discussion of this topic, see Chapter VII below. Footnote added by the author.
679 Recital 7 5AMLD.
680 COM (2016) 450, p. 22. See also European Economic and Social Committee 13666/16, p. 4.
681 On January 3rd, 2018, one bitcoin was exchanged for ca. EUR 12.930 or ca. USD 15.048. Statistics from https://www.coinbase.com/charts, last accessed 3 January, 2018.

laundering Directive is to be amended by explicitly including virtual currency exchanges and wallet providers into the list of obliged parties, and article 3 4AMLD is to be amended to include a definition of virtual currencies. The definition proposed by the Commission reads as follows:

> "'virtual currencies' means a digital representation of value that can be digitally transferred, stored or traded and is accepted by natural or legal persons as a medium of exchange, but does not have legal tender status and which is not funds as defined in point (25) of Article 4 of the Directive 2015/2366/EC[682] nor monetary value stored on instruments exempted as specified in Article 3(k) and 3(l) of that Directive."[683]



The text of the Commission's proposal of the fifth Anti-money laundering Directive mentions that the Commission has examined six different options with regard to the monitoring of activity on virtual currency platforms. The text of the draft Directive however limits itself to a discussion of the system of voluntary self-identification and does not further specify the other possible avenues examined regarding monitoring of transactions within the virtual currency environment and the identifiability of users of the system.[684]

The introduction of clear and certain rules concerning exchanges and wallet providers would indeed be a great step ahead to create legal certainty for those businesses and their customers. Particularly the uncertainty of the applicability of the rules in the fourth Anti-money laundering Directive to those entities was a risk for service providers, as they could not be sure of how the existing rules would be interpreted. Therefore, although the measures are burdensome for service providers, that burden is likely preferable to the uncertainty under which they now operate. This approach has also found support among other stakeholders. The Romanian Chamber of Deputies, for instance, notes that it

682 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127. Footnote added by the author.

683 Proposed text of Article 3 (18) 5AMLD in COM (2016) 450. See also Bonaiuti (2016), p. 36 f.

684 COM (2016) 450, p. 9. See also Pesch/Böhme (2017), p. 96 f.

> "Supports approaching the alternative systems of funds transfer by finding a balance between the protection of the legitimate use of those systems and combating their abusive use for the purpose of money laundering and terrorist financing".[685]

It is not clear, however, how the Commission envisages the monitoring of the blockchain and how Financial Intelligence Units are to be put into a position to identify users carrying out a transaction observed on the blockchain.[686] The proposal of suitable systems to realise these advances is postponed to the 26th of June 2019, when the Commission is obliged to submit its report on the implementation of the fourth Anti-money laundering Directive, pursuant to article 65 4AMLD.[687] However, a system of voluntary self-identification of users of the virtual currency environment would appear to be unlikely to succeed, in particular with the view of identifying criminal users.

## d. Impact on Informal Value Transfer Systems

The impact of the European anti-money laundering framework on informal value transfer systems is similarly difficult to gauge as the impact on virtual currency systems. The Hawala system has proven itself to be remarkably resilient; the Hawala system is accessible in remote and conflict regions as well as in regions where the service is outright forbidden.[688] Hawaladars are fully capable of providing their services underground and out of sight of the authorities. The effectiveness of anti-money laundering measures on hawaladars and the system as a whole has not been demonstrated.

Indeed, hawaladars are somewhat easier to classify under the terms of the Anti-money laundering Directive than providers of virtual currency systems. A hawaladar's services are based on cash, the classification of which as property is not an issue. Hawaladars may also themselves be classified as obliged entities. However, as has been mentioned, the effectiveness of the measures may be questioned. Just as with virtual currencies, there are several issues hampering the effective

685 Romanian Chamber of Deputies, 13576/16, p. 4.
686 See also Hendrickson/Hogan/Luther (2014), p. 5 f.
687 COM (2016) 450, p. 38 f.
688 Ryder (2007), p. 827 f.

and thorough application of anti-money laundering measures to the services of hawaladars. These are especially the fact that Hawala is a system often used within a certain context of a cultural community, and is often inaccessible to persons outside of this community. This closed character makes it easier for hawaladars to keep out of sight of the authorities. Furthermore, the global nature of a Hawala network is confronting the European lawmaker with the same difficulties as the global nature of virtual currency systems.

This section is going to examine first the means Hawala offers for a money laundering operation. In the following subsection, the challenges faced by regulators, briefly mentioned above, will be further explained. The last two sections specifically discuss the classification of hawaladars as obliged entities under the Anti-money laundering Directive, and trace the application of the obligations which hawaladars therefore have to comply with.



**i. Money Laundering through Hawala**

In the discussion of Hawala in the previous chapter, Hawala has been sketched primarily as an alternative means for expatriate communities to send remittances from Europe to countries in which Hawala is one of the primary channels for financial transfer. The reasons why members of these communities would wish to use Hawala rather than the formal banking sector have been discussed in detail.[689] In the following sections, however, another user group of the Hawala services will be discussed: that of persons wishing to use these services as a means for money laundering or terrorist financing.

Hawala is relatively easy to use for money laundering operations. The placement stage is particularly easily accomplished with the means of Hawala. It has already been mentioned that many hawaladars keep the costs of their services low by avoiding high overhead costs, which many of them do by combining their business as a hawaladar with keeping a shop, or another business providing services. Therefore, a hawaladar can usually easily explain the cash generated by his Hawala services as proceeds of this business, or use it to pay for expenses generated by that business.[690] If the hawaladar does not solely concentrate on remittances but also

689 See section (e) of Chapter III above.
690 Jost/Sandhu (2000), p. 12.

services transactions in the opposite direction, some of the cash deposited to be sent by customers will also be paid out to other customers receiving funds.

The second stage, layering, is also easily managed when using Hawala, simply because the level and quality of record keeping applied by a hawaladar is much lower than the records kept by the formal banking sector. Furthermore, as *Jost and Sandhu* point out, if

> "invoice manipulation is used, the mixture of legal goods and illegal money, confusion about 'valid' prices and a possibly complex international shipping network create a trail much more complicated than a simple wire transfer."[691]

The final stage of money laundering, integration, is then in comparison not quite as simple in Hawala as the other two stages. While Hawala allows for criminal money to be moved quickly over long distances and at low risk of detection, additional steps are necessary to transform the cash into investments or into property.[692] This is at least the case in economies which are not predominantly cash-based. While the origin of the cash is very effectively concealed through Hawala in the layering stage, the criminal is still left with large amounts of cash, which can cause suspicion even lacking a traceable connection to its criminal origin. The very effective means of moving funds provided by Hawala does, however, facilitate any further steps taken toward integration.[693]

**ii. Regulatory Challenge**

Hawala has been targeted heavily, especially in connection with terrorist financing, after the attacks of September 11th, 2001. The response to those attacks specifically targeted Hawala as a means by which the terrorist attacks had been facilitated, but it should again be pointed out very specifically that the official report did not find any conclusive evidence that this was indeed the case.[694] Indeed, the 9/11 Commission believes that the formal banking system was used to fund those

691 Jost/Sandhu (2000), p. 12.
692 Note that such conversion may not be necessary in cash-based economies outside of North-western Europe, making Hawala an even more attractive tool for such operations.
693 Jost/Sandhu (2000), p. 13.
694 The *9/11 Commission*, quoted in Redin/Calderón/Ferrero (2012), p. 8.

attacks.[695] Evidence that Hawala was used directly in order to finance terrorist attacks has been obtained, but in those quoted cases, the attacks and the financial operation both were carried out in areas where Hawala is one of the primary channels for financial transactions.[696]

The suspicion against Hawala of being a means for terrorist financing has, despite the lack of formal evidence, led to severe action against that channel, both in the United States and in Europe. While hawaladars previously advertised their services rather openly,[697] the severe action against all Hawala services in response to the terrorist attacks caused an almost collective shift of hawaladars underground.[698] This shift in turn strengthened the belief that Hawala was "secretive by nature",[699] and "politicians, law enforcement agencies and the media declared it as a 'financial tool of terrorism'."[700]



Therefore, the regulatory response to Hawala in the United States and Europe should always be seen in the context of this heavy prejudice against it. However, there have also been less agitated attempts to regulate Hawala. The problem with regulating Hawala appears to be rooted in the imperfect understanding of what Hawala is and how it precisely works, coupled and amplified by this prejudice already shown.

One of the core differences between Hawala and the conventional banking sector lies in the difference of guaranteeing for the security of the financial services offered. In the conventional banking sector, the security of financial transactions is ensured by a large body of regulations,[701] consisting of minimum capital requirements, oversight mechanisms, and disclosure obligations, as well as judicial sanctions, ranging from fines to imprisonment for executive officers responsible for mismanagement. This way of securing the financial services offered by the conventional banking system appears to be acceptable to the majority of the users of this service. It is, however, not the only possible way of ensuring the safety

695 Ryder (2007), p. 827 f.
696 Ryder (2007), p. 827 f. See also Sharma (2006), p. 116 f.
697 Ryder (2007), p. 827 f.
698 Bures (2015), p. 230 f.
699 *Wheatley* quoted in Ryder (2007), p. 826. See also Lennon/Walker (2009), p. 41.
700 Ryder (2007), p. 827. See also BMF (2004), p. 86 f.; Razavy/Haggerty (2009), p. 150.
701 Redin/Calderón/Ferrero (2012), p. 19; Johnson (2011), p. 155. See also Marin (2009), p. 929 ff.

of financial transactions, as shown by the radically different approach taken by hawaladars and their customers.[702]

As has already been explained previously, hawaladars often operate without a license, and out of sight of the official authorities.[703] However, a hawaladar's customers trust in the security of transactions carried out with the help of a hawaladar, because the hawaladar vouches for the security of the transaction with his personal reputation.[704] This way of securing a transaction is accepted by the majority of the users of Hawala. As *Redin, Calderón and Ferrero* aptly summarize, "The regulatory mentality of the West is based in the absence of trust, whereas that is not true for Hawala, in which financial relationships are grounded on the trustworthiness and the reputation of the individual rather than contract."[705] Both approaches have their advantages and disadvantages, and each likely seems very strange to the followers of the other. It is clear, however, that imposing the same approach to both by regulatory action would be "doomed to fail."[706]

This reality has not yet been fully realized by the different entities attempting to regulate Hawala.[707] There are as yet no exceptions for Hawala, or indeed express references to Hawala, in the law in any European directive, though the financial sector is heavily regulated by the European lawmaker.[708] Such special regard for Hawala would, however, be very useful to ensure that vulnerable segments of society are not excluded from financial services. As *Lennon and Walker* observe concerning the inclusion of Hawala in the anti-money laundering legislation of the United Kingdom, "present measures have proven not only to be ineffective but in addition cause extreme hardship when, where there is no formal banking system, the sole method of transferring monies is interrupted."[709]

---

702 Razavy/Haggerty (2009), p. 146 f.
703 Borgers (2009), p. 160 ff.
704 Redin/Calderón/Ferrero (2012), p. 13; Razavi (2005), p. 285.
705 Redin/Calderón/Ferrero (2012), p. 19.
706 Redin/Calderón/Ferrero (2012), p. 19. See also Sorel (2003), p. 377; Ryder (2007), p. 828 f.; Johnson (2011), p. 155; Marin (2009), p. 929 ff.
707 IMF (2005), p. 19 f.
708 BMF (2004), p. 85 f. See also Mezzana/Krlic (2013), p. 5; Marin (2009), p. 929 ff.
709 Lennon/Walker (2009), p. 41. See in this context also Razavy/Haggerty (2009), p. 151; Tridimas (1999), p. 77.

The problem of the exclusion of informal value transfer services appears, however, to have been recognized by the Commission.[710] The proposal for the fourth Anti-money laundering Directive 2015/849 contained a short section on financial inclusion, in which the Commission recognizes that "the fact that applying an overly cautious approach to anti-money laundering and combating terrorist financing safeguards might have the unintended consequence of excluding legitimate businesses and consumers from the financial system".[711] The Commission goes on to state that

> "Work has been carried out on this issue at international level to provide guidance to support countries and their financial institutions in designing anti-money laundering and combating terrorist financing measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime."[712]



More detailed information on the content of this work has not been forthcoming, however.

On the international level, there have been several attempts at regulating Hawala, including in countries where this system is much more prominent than in the United States and in Europe. There are several problems hampering the development of an effective regulatory response. In the first place, as has already been explained, international instruments and recommendations, particularly by the FATF, are primarily fashioned for the conventional banking sector, and largely disregard the need for exceptions and a more flexible approach for the accommodation of informal value transfer systems.[713] Applying this sort of regulation to hawaladars is seen as an example of "Western ignorance",[714] and has proven itself ineffective in several instances A prominent example is supplied by Pakistan, where a complete ban on Hawala appears to have only mildly inconvenienced hawaladars,[715] if at all. Furthermore, there are many communities worldwide, which exclusively rely on Hawala for financial services. Those communities have naturally not been

710 European Commission (2004), p. 6 f.
711 COM(2013) 45 final, p. 5. See also Razavy/Haggerty (2009), p. 150 f.
712 COM(2013) 45 final, p. 5
713 Ryder (2007), p. 827 f.; Johnson (2011), p. 155 f.
714 Razavi (2005), p. 278. See also Ryder (2007), p. 828 f.; Johnson (2011), p. 156.
715 Ryder (2007), p. 827 f.

interested in enforcing regulations against Hawala with much zeal.[716] The fact that authorities particularly in the United States have been quick to condemn the entire Hawala system as a system inextricably linked to Islamic extremism and terrorism also appears to have caused some resentment in the international community.[717] In sum, any regulation of Hawala is thought to only "place an additional administrative burden on financial sector regulators"[718] without tangible results.

### iii. Hawaladars as Obliged Entities

Despite this justifiable doubt of the effectiveness of applying the anti-money laundering legislation to Hawala, the current incarnation of the law does cover hawaladars, if the hawaladar can be fit into one of the categories of obliged parties presented by the Anti-money laundering Directive.

Despite the changes introduced by the fourth Anti-money laundering Directive in other areas, the rules applicable to hawaladars have remained largely unaltered compared to the earlier legal situation. The Directive applies to 'financial institutions', which are defined as undertakings other than credit institutions which carry out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms.

The fourth item in the list contained in Annex I of this Directive mentions 'payment services as defined in Article 4 (3) of Directive 2007/64/EC', which cryptically defines a 'payment service' as 'any business activity listed in the Annex', and that annex finally lists especially 'money remittance' in point (6), and a number of different payment transactions in points (4) and (5). Why a term so central to the anti-money laundering framework as 'financial institution' could not be defined clearly in the newly amended Anti-money laundering Directive is not clear, especially as article 3 4AMLD already contains a paragraph on financial institutions with six subsections. Tangled legal jargon such as this certainly does not help with ensuring that the obligations under the Anti-money laundering Directive are complied with.[719]

716 Razavi (2005), p. 278.
717 Razavi (2005), p. 278.
718 The *IMF* quoted in Ryder (2007), p. 827 f. See also Pieke/Van Hear/Lindley (2007), p. 349.
719 See also IMF (2005), p. 24.

Thus, although the legal construction is exceedingly badly drafted,[720] the final conclusion is that hawaladars are covered by the European anti-money laundering framework as financial institutions (article 3 (2) (a) 4AMLD) and thus obliged entities under the Anti-money laundering Directive 2015/847 (article 2 (2) 4AMLD). This classification, however, comes with a number of obligations, as detailed below.

**iv. Obligations**

Hawaladars generally do not fully comply with their obligations under the anti-money laundering framework.[721]



For instance, the previous chapter started with an example of a Hawala transaction. If one looks a little closer at the transaction, it becomes clear that the transaction is not only between a man and his family, but also a business transaction between two hawaladars. It is unlikely that the hawaladar in Amsterdam asked to see his customer's ID card, or even asked a name if the customer was not previously personally known to the hawaladar. In his books, the transaction will appear as a transaction between himself and the hawaladar in Lahore, noting the date, the amount, and possibly the identity of the recipient or a password, but it may not be necessary that the customer is referenced in the records. The fact that the cash has come into the possession of the hawaladar makes the identity of the sender immaterial to the transaction, as is the case in most cash transactions.

This lack of regard for the identity of the sender and recipient naturally makes Hawala an attractive tool for criminal transactions.[722] Whereas a name and address are attached to both sender and recipient if regular bank accounts are used, the risk of discovery in Hawala is smaller. Other factors that make Hawala interesting for terrorist financing operations and money laundering is the speed of transactions, the low costs, and the accessibility,[723] as the geographic spread of the Hawala network includes the Arabic world, i.e. the areas where Islamic terrorist groups are most active. All these factors combined make Hawala a channel that is vulnerable to abuse by terrorist financing and money laundering operations. Furthermore, the spread of the network over Europe and North America has the consequence,

720 See also European Economic and Social Committee 13666/16, p. 4.
721 IMF (2005), p. 17.
722 Ryder (2007), p. 826.
723 Abramova (2005), p. 103 f.

that the wealthier emigrant communities can more easily and to a large extent undetectedly financially support the terrorist groups of their sympathy.[724]

While there are naturally hawaladars who do follow their obligations under the Anti-money laundering Directive in detail, there are of course also a number of hawaladars knowingly involved in money laundering operations. Alternatively, hawaladars may in some cases not have positive knowledge but reasons to suspect that the funds transferred through their system is of criminal origin. This last group is vulnerable for abuse for money laundering operations. The fact that many hawaladars operate without a licence may make them reluctant to cooperate with the authorities and prevent their reporting suspicious activity. While detecting suspicious activity may be more difficult for a hawaladar than for entities of the conventional banking sector, due to the general lack of automated data processing in a Hawala transaction, suspicion may be formed readily even in the absence of an automated system routinely monitoring all transactions.

For instance, a lot of hawaladars specialise in remittances, which usually do not exceed an amount of EUR 5 000 and occur at intervals of several months.[725] Criminal transactions, however, often require the hawaladar to move hundreds of thousands of euros within a short time.[726] Of course, as has already been mentioned, many hawaladars simply avoid asking questions, and it is likely that the criminals will avoid openly stating the background of the funds. In some circumstances, however, the criminal background of a transaction will be evident. In a case quoted by *Soudijn*, "a courier said that the money he was carrying probably came from the underworld, because 'working persons cannot earn so much money.'"[727]

Reporting such suspicions are therefore a factor in which hawaladar often fall short of their obligations under the Anti-money laundering Directive, and the stated reasons will likely prevent a change in the situation toward an increased level of cooperation and amount of reports. The same applies to identification and record keeping, particularly in a format as required under the terms of the Directive. Hawaladars are therefore also at risk of incurring the penalties for non-compliance, stipulated in the Anti-money laundering Directive.

724 Abramova (2005), p. 102 ff.
725 Soudijn (2015), p. 264 f.
726 Soudijn (2015), p. 264 f.
727 Soudijn (2015), p. 262.

## e. Conclusion

The anti-money laundering legislation is thus primarily written for banks and other entities belonging to what is here called the conventional banking sector. Those entities are all explicitly covered by the Directive, with obligations conferred upon them tailored to match their organisation and features. Alternative systems are not yet explicitly included in the legal framework.

Virtual currencies are going to be included in the fifth Anti-money laundering Directive currently slowly moving through the law-making process,[728] although the potential tangible impact of the proposed rules on virtual currency systems is still anything but clear. The changes primarily concern the explicit inclusion of service providers in the list of obliged entities, which is a change that is to be welcomed as an increase in legal certainty for all parties involved. Other changes, such as a register of voluntarily self-identified users of virtual currencies are likely going to fail.



The situation of Hawala, on the other hand, is not going to be changed significantly with the upcoming amendments to the law, and it can, due to its nature, still potentially easily elude the application of the anti-money laundering framework. Although hawaladars are obliged entities under the terms of the Directive, the application of the strict obligations on hawaladars is hampered by the ease with which hawaladars can offer their services underground and out of sight of the authorities.

This chapter has thus answered the sub-research question concerning the applicability of the anti-money laundering framework to alternative transactions systems. The classification of both Hawala and virtual currencies in the terms of the Anti-money laundering Directive is therefore difficult, but not impossible.

Some features of the customer due diligence regimes are, however, not consistently applied in alternative transactions systems, either because the features cannot be applied, as is the case with monitoring in virtual currency systems, or because the features will not be applied, as is the case with reporting in informal value transfer systems. A follow-up question one might ask oneself in regard to the fact

728 Hildner (2016), p. 492 f.

that some features of the customer due diligence regime are applied to a lesser degree or with less consistency in alternative transactions systems than in the conventional banking sector, is therefore, whether the use of these alternative transactions systems may provide enhanced privacy protection to their users compared to the conventional banking sector. This question will be discussed and answered in Chapter IX, after a thorough examination of the concepts of privacy and data protection, identity, and anonymity.

This concludes the first Part of this thesis, which has provided the background on the anti-money laundering law and on the different conventional and alternative transactions systems.

# PART B

# THE ANALYTICAL FRAMEWORK: PRIVACY, DATA PROTECTION, AND IDENTITY

# Chapter V

## The Rights to Privacy and Data Protection

## Outline:

a. Introduction
b. Primary Sources of Law
    i. The Protection of Private and Family Life under the European Convention on Human Rights
    ii. Conditions for Limitation of the Right to Respect for Private and Family Life
    iii. The Rights to Privacy and Data Protection in the Charter of Fundamental Rights of the European Union
    iv. Conditions for the Limitation of the Rights to Privacy and Data Protection
c. Secondary Sources of Law
    i. Convention C108
    ii. The General Data Protection Regulation
    iii. The Police and Criminal Justice Authorities Directive
    iv. Applicable Framework
d. The Protection of Privacy and Personal Data
    i. Privacy and Private Life
    ii. The Theory of Spheres
    iii. Privacy and Human Dignity
    iv. Personal Data
    v. Categories of Sensitive Data
    vi. Financial Data
    vii. The Principles of Data Protection
    viii. Rights of the Data Subject
e. Measures of Mass Surveillance
    i. Definition
    ii. Chilling Effects
f. Conclusion

## a. Introduction

The second part of this thesis, concerning the framework within which the main research question is to be answered, commences with a thorough explanation of the rights to privacy and data protection. Furthermore, the concept of identity, and the closely related concept of anonymity will be discussed in this second part, in Chapters VI and VII below.

In the previous part of this thesis, the focus lay on one area of criminal law and the prevention of, and investigation into, two specific financial crimes. Considerable weight has been placed by the regulator on combating these particular crimes. In the first place, private businesses in the financial industry are integrated into the anti-money laundering approach by obligating these entities to identify customers, monitor transactions, report suspicious transactions, and retain data. In the second place, law enforcement agencies have been supplied with ample powers of investigation. These powers are to a large extent connected to the analysis and evaluation of the stream of suspicious transactions reports forwarded by financial services providers.



Such powers are, however, always tempered by human rights.[729] The processing of such amounts of data concerning every member of the population of course raises privacy and data protection concerns.[730] The purpose of this chapter is therefore to discuss the content of the rights to privacy and data protection. A thorough discussion of these rights is necessary in the context of this thesis in order to be able to connect these rights to the anti-money laundering measures in the final part of this thesis.

While everyone has an idea of what the terms privacy and data protection mean, the definition of those terms needs some clarification. In the first place, in colloquial use, the term 'privacy' can be defined as "[t]he state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion", as the Oxford English Dictionary defines the word.[731] The word privacy has a long tradition in the English language, having

729 See in this context also historically Jellinek (1901), p. 78 ff.; Edwards/Howells (2003), p. 233.

730 Schertz (2013), p. 722.

731 Oxford English Dictionary, Third Edition 2010, s.v. "privacy". See also Leith (2006), p. 111; Gavison (1984), p. 364.

been in use at least since the sixteenth century.[732] Data protection, on the other hand, is a newer term which has been coined when electronic data processing systems achieved a wider application in the second half of the 20th century. The Oxford English Dictionary defines data protection as follows: "The protection of data from corruption, destruction, or misuse; spec. the legal regulation of access to and use of personal data, esp. that held on computers."[733] It will be seen in the following sections, however, that the definition of these terms is not quite so simple.

Data protection and privacy rights have grown over decades into the shape in which they are applied now. The right to privacy is connected to very old principles such as the secrecy of communications, correspondence, and letters,[734] which has been protected in many countries since at least the seventeenth century, and the inviolability of the home and the protection from illegal search and seizures.

This chapter is organised in such a way that the protection of privacy and personal data can be delineated in increasing detail as the chapter progresses. In this way, the primary sources are described first in section (b), followed by a discussion of the three most important secondary sources in (c), being Convention 108, the GDPR, and the Police and Criminal Justice Authorities Directive. After introducing these legal instruments, the concepts contained therein are to be examined in detail in section (d), discussing in particular the concepts of privacy and personal data, as well as the principles of data protection and the rights of the data subject. Finally, section (e) will briefly discuss the phenomenon of mass surveillance.

## b. Primary Sources of Law

The protection of privacy has a long history,[735] gradually sharpening in focus into a human right recognised across Europe and increasingly in other parts of the

732 Oxford English Dictionary, Third Edition 2010, s.v. "privacy". See for example *Shakespeare's* Troilus & Cressida, published in 1602, Act III scene iii: "ACHILLES. Of this my privacy I have strong reasons. ULYSSES. But 'gainst your privacy the reasons are more potent and heroical." See also De Hert (2003), p. 56.
733 Oxford English Dictionary, Third Edition 2010, s.v. "data protection".
734 Diggelmann/Cleis (2014), p. 442. See also Solove (2002), p. 1142.
735 See in this context also Westin (1984), p. 59 ff.; Nelson (1917), p. 212 ff.

world.[736] This section will begin with two early influential examples of advocacy of a right to privacy. In the first place, *James Fitzjames Stephen* articulated an argument for privacy in 1874.

> "Legislation and public opinion ought in all cases whatever scrupulously to respect privacy. To define the province of privacy distinctly is impossible, but it can be described in general terms. All the more intimate and delicate relations of life are of such a nature that to submit them to unsympathetic observation, or to observation which is sympathetic in the wrong way, inflicts great pain, and may inflict lasting moral injury. Privacy may be violated not only by the intrusion of a stranger, but by compelling or persuading a person to direct too much attention to his own feelings and to attach too much importance to their analysis. The common usage of language affords a practical test which is almost perfect upon this subject. Conduct which can be described as indecent is always in one way or another a violation of privacy."[737]



On the other side of the Atlantic, *Louis Brandeis* and *Samuel Warren* in their pivotal 1890 essay have stated so fittingly,

> "Of the desirability — indeed of the necessity — of some such protection, there can, it is believed, be no doubt. […] The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[738]

736 Schmale/Tinnefeld (2017), p. 346.
737 Stephen (1874), p. 106. See also Schoeman (1984a), p. 10 f.
738 Brandeis/Warren (1890), p. 196. See also Schoeman (1984a), p. 14 f. It should be noted that this thesis is not the place where differences between European and American perspectives of privacy and data protection are to be contrasted. See in this context also Ballard (2013), p. 111; Posner (1984), p. 335 f.; Solove (2002), p. 1099 f.; Edwards/Howells (2003), p. 233.

Those thoughts have gradually developed into the rights to privacy and data protection, recognized as a human right in Europe.[739] This right is recognized in article 8 of the European Convention on Human Rights (the ECHR), and in articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter).

**i. The Protection of Private and Familiy Life under the European Convention on Human Rights**

The most important international instrument covering data protection and privacy within the realm of the Council of Europe is of course the ECHR. It has been of unparalleled value in creating the environment and paving the way for a proper protection of the rights to privacy and data protection as human rights. It was furthermore the primary influence in the development of a system of human rights within the European Union. The Council of Europe adopted the European Convention of Human Rights in 1950, entering into force in 1953. The European Court of Human Rights was established in Strasbourg in 1959 to watch over the Convention.

The ECHR contains a rather broad article 8, which, in its first paragraph, enshrines the right to respect for private and family life:[740]

> (1) "Everyone has the right to respect for his private and family life, his home and his correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

It is striking that the ECHR speaks of the protection of 'private life'. The early set-up of the right to privacy was a defensive right with initially ill-defined borders. However, the content of the right to respect of one's private life was soon brought into sharper focus with the case law of the ECtHR. As the Article 29 Working Party explains,

739 Article 29 Working Party Opinion 14/2011, p. 10. See also Doi (1986), p. 107 ff.
740 See also Article 29 Working Party, Working Document 1/2016, p. 5; Lioy (1891), p. 9 ff.

> "With the increase of new technologies and surveillance possibilities, both in the public and in the private sector, [it] became apparent that there needed to be further protection for individuals from third parties (particularly the State) in addition to 'defensive' rights recognised under Art. 8 of the ECHR by ensuring that [t]he individual had the right to control his/her own personal data."[741]

This right to data protection growing out of this sentiment was first set down in an international instrument in Convention 108 in 1985.[742] Convention 108 was rather a success: It is ratified by all EU Member States and is recognised as a particularly "important source of inspiration"[743] for the Data protection Directive 95/46/EC,[744] which was passed ten years later.

Article 8 of the ECHR is the starting point out of which, some fifty years later, articles 7 and 8 of the Charter grew.[745] The right to respect for private life has grown with the Court's case law of the past half century into a strong protection of privacy and personal data of individuals who can rely on the rights contained in the Convention. The ECHR and the Court's case law have been immensely important for the development of those rights, and continue to play that pivotal role especially in the countries which are part of the ECHR but not Member States of the European Union. In the Member States of the European Union, the Charter of Fundamental Rights of the European Union is slowly beginning to outshine the ECHR in importance.[746]



**ii. Conditions for Limitation of the Right to Private and Family Life**

The ECHR and Convention 108 contain both detailed rules and provisions as well as general principles which have to be complied with. These principles are generally acknowledged to be the core principles of data protection law in Europe, and they are reflected and reiterated in each of the legal instruments.

741 Article 29 Working Party, Opinion 1/2014, p. 3. See also Leith (2006), p. 115.
742 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 01/10/1985.
743 Article 29 Working Party, Opinion 1/2014, p. 3. See also European Commission (1999), p. 22 f.
744 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.
745 Article 29 Working Party, Opinion 1/2014, p. 3.
746 As exemplified by the stronger position of the CJEU to enforce its judgments against offending Member States, and the recent string of case law in which the CJEU used this power to afford stronger protection of personal data and privacy. See for more details Chapter VIII below.

The principles handled by the ECtHR are rather basic, and listed in article 8 (2) ECHR. This second paragraph of this provision, setting out the conditions for limitation of these rights, reads,

> "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[747]

The paragraph thus lists the three core principles for the lawful limitation of the right to privacy, which are (1) in accordance with the law,[748] (2) pursuing a legitimate interest, and (3) necessary in a democratic society.[749]

In the first place, therefore, any interferences must be *in accordance with the law*. This term has been clarified in case law by the ECtHR.[750] The Court has held "that the interference must have some legal basis in domestic law.[751] Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable".[752] In a different judgment, the court has clarified that "a rule is 'foreseeable' if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct".[753]

How clear and foreseeable the consequences of the interference is depends on the circumstances of the case in question. In some fields, the consequences will always be less foreseeable for the average citizen, such as in the case of national security measures.[754] In sum, an interference satisfies this first criterion if it has a basis in

747 See also Fried (1984), p. 213 f.; Uerpmann-Wittzack/Jankowska-Gilberg (2008), p. 85.
748 For more detailed information, see Feiler (2010), p. 9.
749 For an elaboration on this point, see Barak (2013), p. 252.
750 Article 29 Working Party, Working Document 1/2016, p. 7 ff. See also Kilkelly (2003), p. 25.
751 Kilkelly (2003), p. 25 f. Footnote added by the author.
752 ECtHR Case of *Leander v. Sweden* [1987], paragraph 50. See also Korff (2014), p. 89; Kilkelly (2003), p. 25.
753 ECtHR Case of *Amann v. Switzerland* [2000], paragraph 56.
754 ECtHR Case of *Leander v. Sweden* [1987], paragraph 51. See also Article 29 Working Party, Opinion 1/2014, p. 5 f.; Korff (2014), p. 107 f.; Feldman (1999), p. 134; Barnard-Wills (2013), p. 172.

law, and if that law contains a well-defined provision specifying the conditions for the interference. In addition, if the authorities are provided with a degree of discretionary power, the limits of this discretion should be clearly defined, including rules on the proper exercise of this power and legal safeguards against abuse.[755]

Secondly, *a legitimate interest* "may be either one of the named public interests or the rights and freedoms of others."[756] The condition of a legitimate aim is closely related to the justification of an interference in the proportionality test of European Union Law. The legitimate aims explicitly mentioned in article 8 (2) ECHR are "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." This particular justification is rarely a problem in case law, as the term 'legitimate aim' is interpreted very widely by the Court.[757]



Finally, a measure must be *necessary in a democratic society*, which in short "implies that the interference corresponds to a pressing societal need and, in particular, that it is proportionate to the legitimate aim pursued."[758] The term 'necessary' is an indication of the principle of proportionality as applied by the ECtHR. This particular criterion is discussed in detail below in Chapter VIII, in which the case law of the ECtHR is examined to trace the evolution of the principle of proportionality under the ECHR.

The notion of a democratic society is more difficult to discern. The Court has not given a conclusive interpretation of this term, but in case law, "the Court spoke of tolerance and broadmindedness as two of the hallmarks of a democratic society."[759] In addition, "the importance of the rule of law in a democratic society and the need to prevent arbitrary interferences with Convention rights" have been highlighted.[760] However, the precise meaning of the term continues to be elusive and is applied on a case-by-case basis.

755 Article 29 Working Party, Opinion 1/2014, p. 6.
756 FRA Handbook on European data protection law (2014), p. 64. See also Kilkelly (2003), p. 30.
757 Kilkelly (2003), p. 30. See also Chapter VIII below.
758 ECtHR Case of *Leander v. Sweden* [1987], paragraph 56. See also Kilkelly (2003), p. 30 f.
759 Kilkelly (2003), p. 31. See also Uerpmann-Wittzack/Jankowska-Gilberg (2008), p. 85.
760 Kilkelly (2003), p. 31. See also Holaind (1899), p. 154; Barak (2013), p. 226 ff.

### iii. The Rights to Privacy and Data Protection in the Charter of Fundamental Rights of the European Union

The ECHR applies principally within the realm of the Council of Europe. The European Union is to some extent a part of this realm, but also has its own legal instruments. The Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) are the core documents of European Union primary law. Since the entry into force of the Lisbon Treaty (1st December 2009), the Charter of Fundamental Rights stands in line with these two Treaties, enshrining a number of fundamental rights on the European Union level.[761] The Charter shows marked similarities to the ECHR, and is intimately connected to it. Together these two instruments make up the standard of protection of fundamental rights in the European Union.[762] In this way, Article 7 of the Charter simply reads,

> "Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications."

In contrast to the ECHR, this provision in the Charter does not contain a second paragraph with exceptions. Those are contained in Article 52 in a general provision applicable to all rights contained in the Charter.

Next to the right to privacy, the Charter also introduces an explicit right to data protection in the following article 8, which is a novelty compared to the text of the ECHR. This provision reads,

> "Protection of personal data
>
> (1) Everyone has the right to the protection of personal data concerning him or her.
> (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

761 See for the earlier situation Ronellenfitsch (2007), p. 562.
762 Article 29 Working Party, Working Document 1/2016, p. 4.

(3) Compliance with these rules shall be subject to control by an independent authority."

This provision thus puts the right to data protection very clearly on its own feet, and establishes separate rights to privacy and data protection.[763] The second paragraph of the provision mentions some of the most important principles of data protection, which are further defined in secondary law. Finally, the last paragraph demands oversight over the compliance with the rules set out in paragraphs one and two by an independent authority, thereby cementing the establishment of data protection agencies throughout Europe.

**iv. Conditions for the Limitation of the Rights to Privacy and Data Protection**

The scope of articles 7 and 8 is, however, not absolute: The exceptions to all fundamental rights guaranteed in the Charter are contained in Chapter VII of the Charter.



Most of the rights granted by the Charter, such as those rights to privacy and data protection, are formulated in a positive way; they codify a positive right for the inhabitants. Naturally, however, many of those rights must sometimes be limited to allow for the legitimate interests of others. Article 52 of the Charter defines the circumstances under which Charter rights can be limited. The exceptions applicable to articles 7 and 8 of the Charter are, then, again very similar to the exceptions mentioned in article 8 (2) ECHR, and therefore another point of connection between the two documents. Article 52 of the Charter reads as follows:

"Scope of guaranteed rights

(1) Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
(2) Rights recognised by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties.

763 See also Schoeman (1984a), p. 2 f.; Petri (2008a), p. 445.

> (3) In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."[764]

The three conditions for the limitation of a right guaranteed by the Charter are therefore that limitations can only be compatible with the Charter if they are (1) based on a law,[765] (2) do not affect the essence of the right,[766] and (3) comply with the proportionality standard.

The conditions for the limitation of the rights to privacy and data protection are therefore closely related to the conditions for the limitation of the right to respect for private and family life under article 8 ECHR. Only the condition that the essence of a right must be respected is rather different compared to the ECHR. This is an additional safeguard for the protection of the right to privacy and data protection developed in the case law of the CJEU.[767] The specific protection of the essence of a right is to ensure that a right cannot be hollowed out to the extent of becoming meaningless.

## c. Secondary Sources of Law

The protection of the rights to privacy and data protection is further clarified in a number of secondary documents. There are numerous different instruments which come into play in this context, but only some of them have a strong impact in relation to the Anti-money laundering Directive. The most important instruments are, in this context, Convention 108, the GDPR, and the Police and Criminal Justice Authorities Directive. These are here to be shortly introduced before the details of their content, in particular the rights and principles contained in them, are explained in the following sections later in this chapter.

764 See also Schröder (2016), p. 642; Fried (1984), p. 214.
765 Feiler (2010), p. 9.
766 See also FRA Handbook on European data protection law (2014), p. 66.
767 For a more thorough discussion of this principle, please refer to Chapter X below.

**i. Convention C108**

Convention 108 is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[768] Convention 108 is not, strictly speaking, a secondary source of law, though its relationship with the ECHR is sufficiently similar as the relationship between primary and secondary law in European law to be able to subsume it under such a header.

Convention 108 was the first international instrument that contained capable norms concerning the protection of personal data.[769] It was opened for signatures in 1981 and entered into force on October 1st, 1985, therefore predating the first European Data protection Directive 95/46/EC by a decade.[770] It has furthermore to a great extent served as a model for the that Directive and therefore by extension also for the GDPR. In addition, the national law of numerous countries within and beyond the borders of Europe have been strongly influenced by the terms of the Convention. This development cements the Convention's position as "the global gold standard guaranteeing the rule of law" of data protection legislation,[771] of great importance particularly outside of the European Union.



The terms contained within the Convention are very similar but less detailed than those contained in the GDPR. The Convention extends its scope to automatic data processing of personal data by both public and private entities (article 3 C108). Personal data in this context is defined as "any information relating to an identified or identifiable individual" (article 2 (a) C108).

The most notable achievement of the Convention is the establishment of the principles of data protection. Article 5 demands that

> "Personal data undergoing automatic processing shall be:
>
> a. obtained and processed fairly and lawfully;
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

768 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28. January 1981, ETS No.108, entered into force 1. October 1985.
769 See also Greenleaf (2012), p. 68 ff.
770 See also Simitis (1998), p. 2474.
771 Korff (2014), p. 16. See also Ballard (2013), p. 111; Greenleaf (2012), p. 73 ff.

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

An additional principle concerns the adequate security measures to be taken to protect data "against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination" (article 7 C108). Those principles have since become the core content of data protection legislation.[772] They are applied by both the ECtHR and the CJEU,[773] are codified in European Union law, and in being implemented into national law also play a major role in national legislation and case law.

Furthermore, the Convention first set out that special safeguards must apply to sensitive data relating to a person's racial background, political, religious, or other beliefs, health and sex life, as well as, notably, criminal record (article 6 C108).[774] The demand of special safeguards in the processing of sensitive data is also applied in the GDPR.

In addition to the principles of data protection, article 8 of Convention 108 also grants the data subjects a number of rights.

"Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

772 See also the sections on the principles of data protection and the rights of the data subjects in section (d) below.
773 The CJEU applies the principles as contained in the GDPR, which, however, as will be seen in the following sections within this chapter, are closely modelled after article 5 C108.
774 Simitis (1999), p. 1.

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;
d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

As will be seen, equivalents of those rights can also be found in the GDPR, though the rights of the data subject have undergone a more significant development than the principles of data protection. The reason for this lies in a combination of the facts of the early date of the Convention compared to other data protection instruments, and that international conventions are most often less detailed than European regulations.



Finally, the Convention permits exceptions and restrictions to the rights and principles to a surprisingly narrow degree. According to Article 9,

(1) "No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.
(2) Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by law of the Party and constitutes a necessary measure in a democratic society in the interests of:
    a. Protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
    b. Protecting the data subject or the rights and freedoms of others.
(3) Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects."

A clear similarity between the terms of this article and the ECHR can be discerned in the grounds for derogation. Article 8 ECHR protecting the right to a private life contains very similar grounds for derogation, namely "national security, public safety or the economic well-being of the country, for the prevention of disorder

or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." The omission of health and morals from the text of Convention 108 is clearly in line with the increased protection of sensitive data developed since the drafting of the ECHR.[775]

**ii. The General Data Protection Regulation**

Besides the Convention, which all Member States of the European Union have ratified, the applicable secondary law on the level of the European Union in the field must also be complied with by all Member States.[776] European Union secondary law is principally made up of the EU regulations, directives, and decisions. In the field of data protection and privacy, the core framework has been updated as of April 2016, with the General Data Protection Regulation 2016/679 (GDPR),[777] which comprises the core rules of European data protection legislation. The Regulation has been long in coming, with an exceptionally long and difficult legislative procedure and political battle,[778] and was finally passed in April 2016 and is directly applicable in all Member States from May 2018.[779] The GDPR is in essence built with blocks taken from the old data protection framework of Directive 95/46/EC[780] and case law from the CJEU.

The Regulation introduces few fundamental changes to the material data protection framework. The central concept of data protection is that of personal data, which is "information relating to an identified or identifiable person ('data subject')" (art. 4 (1) GDPR). The link between the information and a (natural) person thus stands centrally in the entire architecture of the Regulation, because all information not relating to an identified or identifiable person falls outside of the scope of the GDPR and thus in principle enjoys no protection.

775 For instance, the text of the ECHR stems from a time in which public morals also meant that homosexuality was a criminal offence in most countries across Europe. Convention 108 reflects the development in this regard, in that it not only protects information concerning a person's sex life as sensitive personal data, but also in that it does not allow for derogations from the right to data protection on the ground of the protection of morals.

776 Cannataci (2013), p. 18. See also Chen (2016), p. 311 f.

777 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) OJ L 119, 4.5.2016, p. 1–88.

778 Cannataci (2013), p. 20. See also Schild/Tinnefeld (2012), p. 317; Schaar (2007), p. 260 f.; Van der Sloot (2014), p. 307 ff.

779 Kühling/Martini (2016), p. 448.

780 Roßnagel (2016), p. 564; Reding (2012), p. 119 ff.

A second concept of high importance is that of processing of data. The act of processing is what personal data is to be protected from, which makes a very wide definition necessary. According to article 4 (2) GDPR,

> "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

The natural or legal person in charge of personal data, the data controller, is therefore bound to the provisions of the data protection framework at all times.



The GDPR in principle always applies whenever personal data is processed. In article 2 GDPR, it is put forward that "[t]his regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filling system or are intended to form part of a filing system." The Regulation thus applies whenever personal data are processed in any way. There are few exceptions to the scope of the Regulation, but one notable exception is listed in article 2 (2) (d) GDPR, processing "by competent authorities for the purposes of 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." Processing of personal data by competent authorities for the purposes mentioned falls under the terms of the Police and Criminal Justice Authorities Directive instead.

Processing of personal data is in principle only lawful when the controller has a valid reason (art. 6 GDPR).[781] Those reasons are, among others, that processing is necessary to comply with the law, or that the data controller must process personal data in order to perform a contract between himself and the data subject. In practice, however, the most important legal ground for lawful processing is consent, to the conditions for which article 7 GDPR is devoted.[782]

781 Buchner (2016), p. 157.
782 See in this context Simitis (1998), p. 2477; Kühling/Martini (2016), p. 451; Roßnagel (2016), p. 563; Buchner (2016), p. 158.

Of particular importance is the protection of sensitive categories of data. Article 9 (1) GDPR states that

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

This ban on the processing of sensitive data is not absolute, however.[783] The GDPR in fact doubles the number of exceptions compared to Directive 95/46/EC.

Finally, the GDPR codifies a number of rights of the data subject, among which are the rights to information (art. 13 and 14 GDPR), access to personal data (art. 15 GDPR), rectification (art. 16 GDPR), erasure (art. 17 GDPR), and data portability (art. 20 GDPR). At the end of the text of the Regulation, the remedies, liability and penalties in case of a violation of the provisions of the GDPR can be found. Those penalties have been raised (compared to the earlier Data protection Directive) to administrative fines of up to EUR ten million, or of 2% of the total worldwide annual turnover of a company (art. 83 (4) GDPR).

Several of the notions briefly introduced here will be discussed in detail in later sections within this chapter.

### iii. The Police and Criminal Justice Authorities Directive

It has already been mentioned that the GDPR does not apply to the processing of personal data by law enforcement authorities (art. 2 (2) (d) GDPR). That sector is covered by the Police and Criminal Justice Authorities Directive 2016/680.[784] Law enforcement agencies are not covered by the GDPR but instead by different rules, because the tasks of law enforcement agencies are considered to be of a

783 See also Article 29 Working Party, Opinion 14/2011, p. 26.

784 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

very different nature than those of private undertakings.[785] This different nature is the reason why data protection rules applicable to this sector are also designed differently, as will be outlined briefly.

The Directive maintains the categories of the GDPR concerning personal data and processing. As the GDPR, the Directive applies to all different processing operations of personal data by the controller, with the only difference that the controller in the terms of the Directive must be a 'competent authority'. A competent authority is defined in article 3 (7) of the Directive as

> (a) "any public authority competent for 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; or
> (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of 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".

Important in this context is also the definition of the term processor: "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (article 3 (8) Police and Criminal Justice Authorities Directive).

Notably the two main achievements of the GDPR, namely the extensive rights of the data subject and the support of those rights by considerable penalties, are largely limited or missing from the Police and Criminal Justice Authorities Directive. The Police and Criminal Justice Authorities Directive does contain in article 13 a general right to information relating to the processing of personal data, a right to access (art. 14), and a right to rectification or erasure of personal data and restriction of processing (art. 16).

Those rights are each accompanied by wide limitations. The formula used is largely the same in each of those articles, reading, as in article 13 of the Directive,

785 EDPS Opinion 6/2015, p. 5. See also Cannataci (2013), p. 19 ff.; Schantz (2016), p. 1842.

> "Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject […] to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:
>
> (a) avoid obstructing official or legal inquiries, investigations or procedures;
> (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
> (c) protect public security;
> (d) protect national security;
> (e) protect the rights and freedoms of others."[786]

A similar restriction is repeated in article 15 (1), and article 16 (4). These restrictions correspond to article 39 (1) of the anti-money laundering framework, which restricts any information of a suspicious transactions report to be relayed to the customer.[787]

Finally, while the GDPR contains a catalogue of penalties, including fines of unprecedented magnitude, the Police and Criminal Justice Authorities Directive grants the data subject considerably fewer possibilities in that regard.[788] The data subject principally has the right to lodge a complaint with the supervisory authority (article 52). In other respects, the Directive follows the blueprint of other directives and leaves the provision of remedies up to the Member States, to be treated in the same way as other complaints against law enforcement authorities.

**iv. Applicable Framework**

Connecting the obligations created for obliged entities by the Anti-money laundering Directive with the obligations created for the same parties by the data protection framework generates a mixed picture.[789] In principle, financial services providers are private entities and therefore bound to the obligations of the GDPR.

786 See, however, Korff (2014), p. 107 f.
787 See in this context also the tenth concern discussed in Chapter IX.
788 Article 29 Working Party, Opinion 1/2013, p. 4 f.
789 See also Recital 11 of the Police and Criminal Justice Authorities Directive.

The numerous rights of the customers as data subjects, enshrined in the GDPR, must therefore be guaranteed by the services provider. Furthermore, high fees are set as penalties for non-compliance.[790]

However, in carrying out their duties as obliged entities under the Anti-money laundering Directive, particularly when complying with their duty to report suspicious transactions and complying with requests for information from the FIU, financial services providers also fall into the scope of the Police and Criminal Justice Authorities Directive, as in that capacity, they act as processors of data on behalf of the competent authorities (article 3 (9) of the Police and Criminal Justice Authorities Directive). This is of particular moment, as the processing in that capacity is connected to considerably fewer rights of the concerned data subject.

In addition, large amounts of data are forwarded by obliged entities to the FIUs. FIUs fall into the definition of competent authority, as they are established "in order to prevent, detect and effectively combat money laundering and terrorist financing" (article 32 (1) 4AMLD). While there are differences among Member States as to the organisation of their criminal justice system and where within this system FIUs are settled, all FIUs fall under the definition of competent authorities in the Police and Criminal Justice Authorities Directive under article 3 (7) of that Directive, either under letter (a) or (b).



## d. The Protection of Privacy and Personal Data

### i. Privacy and Private Life

The need for privacy and a protected private life has already been explored at different points in this thesis. However, this section should start with a concise statement on the general desirability of a well-protected right to privacy, as eloquently summarised by *Katerina Hadjimatheou*.

> "Individuals need privacy to build and maintain meaningful relationships, to express their feelings and desires freely in artistic and political ways, and to experiment with and arrive at ideas for themselves about how they want to live their lives. Thus privacy is a condition of both personal

790 Weichert (2015), p. 17.

> happiness and individual freedom […]. Privacy is also a condition of a functioning liberal democracy. Without private space in which to express and exchange political ideas and opinions, explore and practice religious beliefs, teach one's children one's own values and vote anonymously, amongst other things, people's ability to engage in activities of democratic citizenship with genuine autonomy, that is, free of exploitation or oppression, would be weakened […]. This, in turn, would weaken the effectiveness of democracy for society as a whole. For these reasons at least, privacy should be treated as an important value or freedom and should be limited or interfered with only to the extent that is proportionate to the protection of other equally or more important values or interests."[791]

The concept of privacy is one which is still in the process of development.[792] Although it is, legally speaking, a rather new right, the concept has very deep roots. For instance, *Georg Simmel* made the following observations on *secrecy* in 1906:

> "The intention of the concealment assumes, however, a quite different intensity so soon as it is confronted by a purpose of discovery. Thereupon follows that purposeful concealment, that aggressive defense, so to speak, against the other party, which we call secrecy in the most real sense. Secrecy in this sense – i.e., which is effective through negative or positive means of concealment – is one of the greatest accomplishments of humanity. In contrast with the juvenile condition in which every mental picture is at once revealed, every undertaking is open to everyone's view, secrecy procures enormous extension of life, because with publicity many sorts of purposes could never arrive at realization. Secrecy secures, so to speak, the possibility of a second world alongside of the obvious world, and the latter is most strenuously affected by the former."[793]

In these observations, one can already discern an approach to the concept of privacy, and of the moral and legal right to respect for the individual's privacy. However, it was not until the explicit protection of the right to respect for private

791 Hadjimatheou (2014), p. 196. This description is especially useful as it does not only concentrate on the individual in isolation but also brings in the social context in which a person develops their personality. See also Becker/Seubert (2016), p. 74 f.
792 Solove (2002), p. 1088 f.; Schoeman (1984a), p. 2 f.; Kokott/Sobotta (2013), p. 223 ff.
793 Simmel (1906), p. 462. See also Leith (2006), p. 113; Doi (1986), p. 107 ff.; Solove (2002), p. 1105.

and family life in the ECHR that the concept of privacy, and the urgency to protect one's privacy, began taking the shape it has now attained: a human right,[794] closely connected to the inviolable human right of human dignity.[795]

In contrast to the closely mapped-out framework surrounding the concept of data protection, privacy is a term not conclusively defined in law.[796] The concept of privacy is necessarily a term coloured by the personal perceptions of the person using the term.[797] In the words of *Patrick Murck* in the context of virtual currencies,[798]

> "Privacy is many things to many people. Among other things, it is the individual's bulwark against objectification by governments, corporations, and other individuals. People who have their privacy have more personal power and a richer, more independent life. Privacy is also a means to various ends, including personal security and freedom of speech and action."[799]



Similarly, a report from the office of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, used the following definition: "Privacy can be defined as the presumption that individuals should have an area of personal autonomous development, interaction and liberty free from other uninvited individuals."[800] The same report then goes on to clarify the content more closely:

> "The duty to respect the privacy and security of communications implies that individuals have the right to share information and ideas with one another without interference by the State (or a private actor), secure in the knowledge that their communications will reach and be read by the intended recipient alone. The right to privacy also encompasses the right

794 Leith (2006), p. 109.
795 Lynskey (2014), p. 572; Tinnefeld (2007), p. 628; Schertz (2013), p. 722.
796 Leith (2006), p. 111; Solove (2002), p. 1088 f. See Becker/Seubert (2016), p. 74 with references to a number of definitions proposed in literature.
797 Murck (2013), p. 96. See also Simitis (1998), p. 2475; Bull (2006), 1618.
798 In the context of financial privacy granted by the use of virtual currencies.
799 Murck (2013), p. 96. See also Gavison (1984), p. 364 f.
800 United Nations General Assembly, Sixty-ninth session [2014], Agenda item 68 (a), p. 12. See also Böhme-Neßler (2016), p. 5 f.; Thomson (1984), p. 275 f.; Maras (2012), p. 77; Becker/Seubert (2016), p. 74.

> of individuals to know who holds information about them and how that information is used."[801]

As the above descriptions show, the right to privacy protects a subject matter that is much more difficult to grasp and define than the closely related concept of data protection.[802] While the right to data protection protects all data relating to an identified or identifiable person, the right to privacy is not limited to the processing of information, but covers also surrounding and related issues.

The ECHR speaks of the respect to private life rather than of a right to privacy, although the concepts are very closely related. This close relation is also reflected in the difficulties of definition. The ECtHR has consistently held that the diverse nature of the term private life simply does not allow for a single concise definition.[803]

> "The Court notes that the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person […]. It can therefore embrace multiple aspects of the person's physical and social identity […]. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 […]. Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family […]. Information about the person's health is an important element of private life […]. The Court furthermore considers that an individual's ethnic identity must be regarded as another such element […]. Article 8 protects, in addition, a right to personal development, and the right to establish and develop relationships with other human beings and the outside world […]. The concept of private life moreover includes elements relating to a person's right to their image […]."[804]

This abstract summary of some core areas of the term *private life* shows the diversity of the elements of the definition of the concept of *privacy.* It should be

801 United Nations General Assembly, Sixty-ninth session [2014], Agenda item 68 (a), p. 12. See also Simitis (1998), p. 2476.
802 See also Michl (2017), p. 349 ff.; Simitis (1998), p. 2475; Becker/Seubert (2016), p. 74 f.
803 Kilkelly (2003), p. 11. See also Cannataci (2009), p. 9.
804 ECtHR Case of *S. and Marper v. United Kingdom* [2008], paragraph 66. See also Preibusch (2013), p. 1134.

noted, however, that the ECHR and the case law of the ECtHR do not distinguish as sharply between the rights to privacy and data protection as the Charter and the CJEU do.

In this context, literature may fill the gap. *Diggelmann and Cleis* bring a definition of the term privacy down to two 'core ideas', namely that "Privacy is about creating distance between oneself and society, about being left alone (privacy as freedom from society), but it is also about protecting elemental community norms concerning, for example, intimate relationships or public reputation (privacy as dignity)."[805] This definition is helpful, as it creates an accessible and not overly technical concept of the different aspects of privacy. Both of these concepts of privacy, privacy as freedom from society and privacy as dignity, will be applied consistently throughout this thesis.



**ii. The Theory of Spheres**

As has already been shown, privacy is a rather vague concept and therefore demands clarification in many ways. One aspect which needs to be elaborated upon is the intrusions into an individual's privacy can be valued very differently depending on where they take place.[806] For example, most people would surely agree that video surveillance can be justified in public spaces with increased levels of criminal activity, such as around train stations in large cities. But video surveillance at the work place or even at private homes are certainly much more difficult, if at all possible, to justify.[807]

The Theory of Spheres ("*Sphärentheorie*") is a model applied by the German Constitutional Court (BVerfG) to determine the intensity of an interference with an individual's right to privacy.[808] Similar considerations are also applied by the ECtHR and other courts.[809] The theory of sphere is based on the idea that an interference weighs heavier when it comes closer to the private life of an individual,[810] while an interference is more likely to be justifiable when it occurs in

805 Diggelmann/Cleis (2014), p. 442. See also Gurlit (2010), p. 1036; Preibusch (2013), p. 1134; Bloustein (1984), p. 186 f.; Fried (1984), p. 209; Kant (1887), p. 138 f.; Becker/Seubert (2016), p. 74.
806 See also Seubert (2012), p. 101 f.
807 See for a positive take on video surveillance and privacy Birnstill et al. (2015), p. 300 ff.
808 This concept will come into play also in Chapter X below.
809 Kilkelly (2003), p. 35. See also Schwartz (1968), p. 749; Solove (2002), p. 1131.
810 Hadjimatheou (2014), p. 197; Worms/Gusy (2012), p. 93.

the public life of society. For this end, the privacy of individuals is separated into three spheres: the social- or public sphere, the private sphere, and the intimate sphere.[811]

At the outside boundary lies the social- or public sphere. The individual moves in the social sphere whenever he or she takes part in public life.[812] In public life, the individual is exposed to contact with other members of society, can be seen by others when walking on the street or taking a bus, and can be casually overheard when having a chat in a crowded café. The individual will thus usually already adapt his behaviour to social acceptability and accept a certain loss of privacy which comes naturally with the company of strangers. Therefore, interferences with the individual's right to privacy can be most easily justified in the public and social sphere,[813] where it may for example take the shape of video surveillance of public places.[814] However, even in this sphere, the principle of proportionality must be strictly respected.[815]

Closer to the individual's personal life is the private sphere. As the BVerfG put it, it is one of the conditions for the free exercise of an individual's right to privacy that each individual has access to a place in which he can be unobserved to himself or with persons he particularly trusts, without having to regard to social conventions and without fear of public sanctions.[816] The classical place as meant in this context is naturally an individual's own home.[817] Most people will act very differently in their own houses, and in company with friends and family members, than they would in public.[818] This difference in behaviour is based on the fact that individuals are either alone and unobserved, or in the company of persons to which a special relationship of trust exists. Besides friends and family, such a special relationship

811 Some of the literature distinguishes five spheres, (the public, social, private, intimate, and secret spheres). See Schertz (2013), p. 722 f.; Poscher (2009), p. 271.
812 Martini (2009), p. 844. See also Prosser (1984), p. 108 f.; Karg (2013), p. 77.
813 Martini (2009), p. 844.
814 It should be pointed out that this view is not entirely undisputed. See Hadjimatheou (2014), p. 196, with further references.
815 For instance, while procedures before a court are in principle open to the public, in some Member States the press may not report the full name of parties to the cases unless there are special reasons. See for more information on the principle of proportionality Chapter VIII below. See also Schertz (2013), p. 723.
816 BVerfG, 1 BvR 1689/88 [1994], paragraph 20. See also Gurlit (2010), p. 1039.
817 Solove (2002), p. 1137; Hohmann-Dennhardt (2006), p. 546.
818 See in this context also Lioy (1891), p. 9 ff.

of trust may also exist with other persons, particularly medical practitioners.[819] It should also be pointed out that an individual's own home is by no means the only place in which an individual may establish his private sphere. Under certain circumstances, other areas can fall under this category as well, for instance a restaurant or a person's office.[820] Interferences into the private sphere can only be justified exceptionally, under strict observation of the applicable safeguards, in particular the requirement of proportionality.[821]

Finally, and most importantly, the individual has an intimate sphere, an area of particular privacy.[822] There are areas of an individual's private life which he may not wish to share even with the persons who are allowed in his or her private sphere, but which are either completely withdrawn from all other persons,[823] or which are shared only with one's partner, best friends, parent, doctor, and other persons to which an individual has a special relationship of particular confidence.[824] Areas of a person's intimate sphere may be localities such as the bed- and bathroom, but also items such as confidential letters or a diary.[825] This area of a person's private life can in principle not be intruded upon by the state, a consideration of the interests of other persons does not take place.[826] The reason for this particular protection is that this area of a person's private life is so closely connected with that person's dignity, which also cannot be interfered with.[827]

Naturally, these spheres are not clearly delineated, and each person may value each sphere differently.[828] However, the differentiation of spheres does help to determine the intensity of an interference with the individual's personality rights,[829] and in particular with the right to privacy.

819 Martini (2009), p. 844. See also Becker/Seubert (2016), p. 76.
820 Martini (2009), p. 844.
821 Schertz (2013), p. 723.
822 Schertz (2013), p. 723; Maras (2012), p. 77.
823 See in this context Becker/Seubert (2016), p. 74 for some historical background and references to John Locke and John Stuart Mill.
824 See also Gerstein (1984b), p. 268 f.; Reiman (1984), p. 305; Schoeman (1984b), p. 411.
825 Hohmann-Dennhardt (2006), p. 546.
826 Martini (2009), p. 844; Linke (2016), p. 891; Schertz (2013), p. 723. See also Gurlit (2010), p. 1039; Cupa (2012), p. 425 f.
827 Martini (2009), p. 844. See also Bloustein (1984), p. 186 f.; Solove (2002), p. 1116, 1148 f.
828 Martini (2009), p. 844; Buchmann (2015), p. 511. See also Spindler (2012), p. 98 f. on the difficulty of applying the theory of spheres to an online context.
829 Lynskey (2014), p. 590 f.; Hohmann-Dennhardt (2006), p. 546.

### iii. Privacy and Human Dignity

It has already been explained above that the right to privacy, and in particular the intimate sphere of an individual's rights are especially closely connected to the right to human dignity. This particularly close connection is emphasised at different points in this thesis and will play a role in Chapter X, so a few words should be dedicated to the connection between the right to privacy and the right to human dignity.

The connection between the right to privacy and the respect for human dignity has been emphasised both in the literature as well as in case law. In particular the BVerfG has had the opportunity to discuss and emphasise this connection at several occasions. In its jurisprudence, the Court clearly positions itself with the opinion that the 'inviolability' of human dignity does not allow any consideration of the interests of the state or third parties, and is therefore exempted from the application of the proportionality principle.[830] The protection of human dignity must be absolute, and cannot be subordinated under any other interest, not even the public interest in investigating the most serious of crimes:

> "This protection must not be relativized balancing with the interests of law enforcement according to the principle of proportionality […]. There will always be forms of especially grave crime and corresponding situations of suspicion, which may cause the effectivity of law enforcement as a public interest to appear to be of greater importance than the protection of the right to human dignity of the suspect. Such an evaluation is, however, denied to the state by article 1 (1), article 79 (3) GG."[831]

It is clear, therefore, that even the interest in the prevention, detection, investigation and prosecution of serious criminal offences, in particular of terrorism,[832] cannot be balanced against the right to human dignity.[833]

---

830 Martini (2009), p. 844; Linke (2016), p. 891; Schertz (2013), p. 723. See also Gurlit (2010), p. 1039; Baum (2013), p. 584.

831 BVerfG, 1 BvR 2378/98 [2004], paragraph 121. Article 1 (1) GG protects human dignity; article 79 (3) GG protects the fundamental rights and principles contained in articles 1-20 GG from alteration. See also Poscher (2009), p. 270.

832 See in this context CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 51. See also Skouris (2016), p. 1364; Tridimas (1999), p. 77; Solove (2007), p. 411; Waldron (2003), p. 191 f.

833 Poscher (2009), p. 276; Baum (2013), p. 584.

The importance of this fact can hardly be overstated. While other human rights can be limited to a certain extent, in accordance with the principle of proportionality and other applicable safeguards, such limitations are in principle not applicable to the respect for human dignity. Those aspects of a person's privacy that are particularly closely related to a person's dignity must therefore also be exempted from intrusions, even if they may be deemed proportionate. Which aspects those are cannot be defined in general terms, but would need to be determined on a case by case basis. There will, however, be a certain overlap with the categories of sensitive data: information relating to a person's political opinions, religious or philosophical beliefs, and information concerning health or sex life and sexual orientation will often be very closely connected to the most intimate sphere of an individual's life. This information therefore may be directly connected to a person's dignity, and must be especially protected from any interferences.



**iv. Personal Data**

The rights to privacy and data protection are intimately connected. The protection of personal data is essentially an effective way to protect an individual's privacy, but not all of an individual's privacy is related to data.[834] In this and the following sections, personal data and its protection will be in focus.

Any discussion about privacy and data protection must contain a clarification of the term 'personal data', so often used already in this section. The definition used for the term is the definition given in the GDPR in article 4 (1) as well as in Convention 108, in article 2 (a). According to both European law and according to the Council of Europe, personal data is all information relating to an identified or identifiable natural person. The term information in this context is interpreted very widely, covering any sort or type of information, including information concerning objects which are related to a data subject,[835] such as prominently mobile devices or personal computers.

That the person is a natural person is logical when one considers the purpose of privacy rights, which have grown out of the obligation of a state to respect the private lives of natural persons.[836] Therefore, the rights of privacy and data protection can be applied only in a very limited scope, if at all, to legal persons.

834 See on data protection as a human right Tzanou (2013), p. 89 ff.
835 Rückert (2016), p. 19.
836 FRA Handbook on European data protection law (2014), p. 37.

Furthermore, persons no longer in life also do not enjoy privacy rights to the same extent as living persons.[837]

An identified person is, in this context, a person who can be distinguished from everyone else, for instance because the person's name, date of birth, and address are among the information in question.[838] An identifiable person is one whose identity is not clear at first sight, but which can be established with a little effort, for example the person behind a phone number, an IP address, or an automobile license plate number. There is some disagreement among scholars researching data protection and privacy rights, about how far removed the natural person may be from the information which makes him or her identifiable, i.e., how much effort it takes to identify a person.[839] For instance, if the information in question is a phone number, the person behind that phone number is easily identifiable for anyone. If the information in question is a licence plate number, access to information about the holder is already a lot more restricted for some people or entities, while it is just a click away for others.

There are pieces of information which are even harder to place. DNA samples, for instance, are impossible to decipher for an average person, but a person with access to the right equipment would not have any difficulties in analysing DNA and identifying a person based on that analysis. Furthermore, the difficulty of identifying a person based on a given piece of information is shifting. While it would have been impossible for an average person to learn the name of someone they saw in the streets other than by simply asking this person, the soaring popularity of social networks has favoured face-recognition techniques which make it possible for anyone to take a picture of a person and have an application search social media networks until it found a match, thereby revealing, in most cases, not only the name of the person, but also allowing access to the social media profile of that person, revealing in some cases countless additional points of information about that person.

837 FRA Handbook on European data protection law (2014), p. 37.
838 See Chapter VI (c) for a more thorough discussion of the terms direct and indirect identifiability.
839 See in this context for example the case *Breyer* discussed below: CJEU Case C-582/14 *Patrick Breyer* v *Bundesrepublik Deutschland* [2016]. See also Schantz (2016), p. 1842 f.; Knopp (2015), p. 529.

In a recent judgement, the CJEU had the opportunity to shed some light on this aspect of personal data. In the case *Breyer*, the Court was occupied, among other things, with the question whether or not dynamic IP addresses are personal data. The Court sums up the conflict in the following terms:

> "The Bundesgerichtshof (Federal Court of Justice) refers to the academic disagreement relating to whether, in order to determine whether someone is identifiable, an 'objective' or 'relative' criterion must be used. The application of an 'objective' criterion would have the consequence that data such as the IP addresses at issue in the main proceedings may be regarded, at the end of the period of use of the websites at issue, as being personal data even if only a third party is able to determine the identity of the data subject, that third party being, in the present case, Mr Breyer's internet service provider, which stored the additional data enabling his identification by means of those IP addresses. According to a 'relative' criterion, such data may be regarded as personal data in relation to an entity such as Mr Breyer's internet service provider because they allow the user to be precisely identified […], but not being regarded as such with respect to another entity, since that operator does not have, if Mr Breyer has not disclosed his identity during the consultation of those websites, the information necessary to identify him without disproportionate effort."[840]



The Court does come to the conclusion that dynamic IP addresses are personal data, even if they are collected by an entity which is not itself in a position to identify the internet user based on the IP address alone.

> "The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified. Furthermore, recital 26 of Directive 95/46 states that, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. In so far as that recital refers to the means likely reasonably

840 CJEU Case C-582/14 *Breyer* [2016], paragraph 25. See also Schrey/Thalhofer (2017), p. 1433.

> to be used by both the controller and by 'any other person', its wording suggests that, for information to be treated as 'personal data' within the meaning of Article 2(a) of that directive, it is not required that all the information enabling the identification of the data subject must be in the hands of one person. The fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user's internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of Directive 95/46. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject. Thus, as the Advocate General stated essentially in point 68 of his Opinion, that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant."[841]

Personal data can be anonymized if the link between the data and a natural person is completely removed, i.e. if the data no longer relates to a natural person.[842] This condition should be interpreted strictly. If the link is hidden and protected from access, the data is pseudonymised.[843] Anonymous data is, because of the missing link to a natural person, no longer to be considered personal data, while pseudonymous data is still personal data, though the link to a natural person is not immediately accessible.[844]

All of those problems which are only outlined here are going to be discussed in detail in the following Chapters VI and VII.

841 CJEU Case C-582/14 *Breyer* [2016], paragraphs 41-46. See also Schrey/Thalhofer (2017), p. 1433.
842 FRA Handbook on European data protection law (2014), p. 36.
843 FRA Handbook on European data protection law (2014), p. 36.
844 FRA Handbook on European data protection law (2014), p. 36.

**v. Categories of Sensitive Data**

In Convention 108, the drafters of the Convention first set up a special regime for certain sets of data, which should generally not be processed. Most of the categories of sensitive data relate to information which puts the data subject at particular risk of negative consequences, often discrimination.[845] The specific categories of data considered to be sensitive vary to some extent among the instruments, however.

Convention 108 contains the categories of sensitive data in article 6 C108:

> "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."[846]



The system of including a number of particularly sensitive categories of data which are not to be processed has found its way into all other major data protection instruments since Convention 108. One of these major instruments introduced after this Convention was Directive 95/46/EC, the Data protection Directive (DPD), which included a provision on sensitive data in article 8 (1) DPD:

> "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

It can be seen that in an extension of the categories of Convention 108, the Directive includes trade union membership. Article 9 (1) of the GDPR further elaborates on the categories sensitive data by including genetic and biometric data:

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,

845 See Mezzana/Krlic (2013), p. 5.

846 In regard to the data subject's criminal record, it is interesting to note that the ECtHR had found that "the interference with an individual's private life caused by the keeping of records relating to criminal cases of the past is relatively slight", Kilkelly (2003), p. 35. See ECtHR Case of *G.W. v. Federal Republic of Germany* [1962].

> and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

The processing of data falling into any of these categories is in principle prohibited.[847] It could be said that sensitive data is to data protection what the intimate sphere is to the right to privacy.[848] Both of these categories grant especial protection to specific aspects of the rights to privacy and data protection.

Article 10 GDPR also mentions criminal records. Criminal records are not a category of sensitive data, but according to that article, such data can only be processed in the presence of special safeguards.[849] The design of these safeguards is left to the discretion of the Member States.

However, this prohibition of the processing of sensitive categories of data comes with a number of exceptions. Article 6 C108 demands that these data is not processed automatically unless there are sufficient safeguards contained in the national law. The Data protection Directive and the GDPR contain a list of rather broad exceptions in the second paragraph of the provision (article 9 (2) (a-j) GDPR).[850] The exceptions include explicit consent of the data subject, substantial public interests, protection of the vital interests of the data subject,[851] data which are manifestly made public by the data subject,[852] and several other points. These points have been criticised severely, however. In particular the notions of consent[853] and of public interest have been attacked.[854] In the words of Simitis,

> "Sensitivity is reduced to a merely ornamental function where the access can be broadened without any difficulties. Exceptions can certainly not be avoided. But as justified as they may appear, they are intolerable as long as their wording is not precise, their purposes and consequences not

847 Article 29 Working Party, Opinion 14/2011, p. 26. See also Weichert (2017), p. 539.
848 See also Weichert (2017), p. 539.
849 Weichert (2017), p. 541.
850 Simitis (1999), p. 9.
851 See also Schoeman (1984b), p. 404.
852 In this context, see also Prosser (1984), p. 110 f.
853 See also Simitis (1998), p. 2477.
854 Simitis (1998), p. 2479.

> clearly determined, the data asked for not confined to really necessary information and the use limited to unmistakably defined controllers."[855]

The system of categorising certain sets of data as sensitive and prohibiting their processing has received some criticism. In the first place, what data sets a person may consider to be sensitive is a very personal reflection, depending on a data subject's individual situation, preferences and background. Not everyone may consider the categories of sensitive data protected under the GDPR as sensitive, while some people may wish other information about them to be exempted from processing.[856] Secondly, the system of in principle prohibiting the processing of sensitive data, but then tempering this prohibition with a large number of exemptions, appears inexpedient. Instead, a more efficient system may have been designed by strengthening the principle of purpose limitation (article 5 (1) (b) GPDR)[857] and ensuring that sensitive data is processed strictly on a need-to-know basis only.[858] The evolution of all of these concepts is still ongoing, however. It remains to be seen how the Courts will continue to apply the protection of sensitive categories of data.



**vi. Financial Data**

One criticism often made with regard to the protection of sensitive data is that the GDPR prescribes a list of categories of sensitive data. It still remains to be seen whether this list will be considered to be exhaustive.[859] An exhaustive list would have the drawback that it would leave no room for national legislators to reflect cultural traditions or political decisions in including or removing certain categories of sensitive data.[860] For instance, the condition of a data subject's trade union membership may be considered less sensitive in some states than a data subject's criminal record. Under the GDPR, however, the former must be protected as sensitive data across all Member States, while the latter is not included in the categories of sensitive data.

A category not included within the sets of sensitive data is the category of financial data. Financial data is the term encompassing the sum of a data subject's transaction data.[861]

855 Simitis (1999), p. 10.
856 See also Simitis (1999), p. 6 f.
857 See in this context also Grafenstein (2015), p. 790 f.
858 Moerel (2016).
859 Simitis (1999), p. 3.
860 Simitis (1999), p. 6 f.
861 See in this context also Freiling/Heinson (2009), p. 550 f.

Financial data as such is not classified as sensitive data under the GDPR. Its exclusion from this list is, however, not self-evident. Categories of sensitive data are generally protected because of the grave impact this data can have on the data subject. And indeed, a data subject's credit history is something that may have grave consequences for his or her life when it becomes known.[862] Even where a data subject has defaulted on a loan years ago and the situation has been remedied to the mutual satisfaction of the data subject and the counterparty, the previous default may still have an impact on the data subject's estimated creditworthiness and can limit his or her lifestyle choices rather severely wherever these choices are related to finances.

The reason why financial data are not to be classified as sensitive data is likely to be imputed cumulatively to a number of factors.[863] In the first place, the fight against tax evasion and tax avoidance is a policy goal of increasing importance on both the European as well as on Member State level. The fight against tax evasion and avoidance is, however, a fight entirely dependent on financial data, and on the extensive processing and mining thereof. These processes would be prima facie prohibited by the inclusion of financial data into the categories of sensitive data, although the public interest exception contained in article 9 (2) (g) GDPR would extend to cover the activities of tax authorities. In the second place, and closely connected to the reason named previously, the fight against terrorist financing and money laundering should be considered. Just as the fight against tax evasion and avoidance, anti-money laundering and the fight against terrorist financing both depend largely on the processing of financial data, a policy goal which is not to be hampered by any substantial restrictions. Those two primary reasons are also closely connected to the financial well-being of the state, which is an express derogation under article 8 (2) ECHR. In the third place, financial service providers have an interest in being able to process financial data with as few hindrances as possible.[864] The processing of data is, indeed, the overarching business interest of the financial sector, and any restrictions on this processing would be seen as injurious.

862 See also Rachels (1984), p. 291.
863 Frasher (2016), p. 9 f.
864 Simitis (1986), p. 190.

However, it is clear that financial data can often reveal sensitive information about a data subject. In this way, a person's transaction history may contain information relating to a person's political opinions, or religious or philosophical beliefs, by showing donations to a political party, church, or foundation. It may show an individual's trade-union membership by revealing the deduction of monthly or quarterly membership fees. Finally, data concerning health or sex life may be contained in a person's transaction history, if medical costs are deducted from this person's account, if certain significant purchases were made, or if that person has made card payments at certain establishments. All of this data is undoubtedly sensitive, and should therefore be protected with special safeguards.

### vii. Principles of Data Protection

Principles of data protection were first developed in Convention 108, as has already been shown above.[865] The GDPR to a large extent adopted these principles and then continued to develop them, resulting in a detailed framework of data protection principles, with which any processing of personal data must comply.[866] There are six key principles of European data protection law, enumerated in article 5 GDPR. Most of those principles are repeated in article 4 of the Police and Criminal Justice Authorities Directive in similar wording, with some notable exceptions.



The first principle is *the principle of lawfulness, fairness, and transparency*, mentioned in article 5 (1) (a), which sets out that all personal data must be "processed lawfully, fairly, and in a transparent manner in relation to the data subject".[867] This first principle is at once also the central principle, setting out the terms of data processing. It is closely related to the protection of privacy and personal data in article 8 ECHR and articles 7 and 8 of the Charter, as it directly relates to the primary conditions that must be met by any limitations to those rights.[868] In contrast to the GDPR, the Police and Criminal Justice Authorities Directive notably omits the latter sub-clause concerning transparency (art. 4 (1) (a) of the Directive). This is directly related to the access rights of the data subject,

865 See also Hornung/Schnabel (2009a), p. 87 for the role the BVerfG census decision played in their development.
866 Bizer (2007a), p. 350 f.
867 See, in this context, also Schwartz (1968), p. 742; Roßnagel (2016), p. 563.
868 Article 29 Working Party, Opinion 1/2014, p. 15. See also the discussion on proportionality in Chapter VIII below.

which are considerably limited in the Police and Criminal Justice Authorities Directive compared to the GDPR.[869]

The second principle is *the principle of purpose limitation* (article 5 (1) (b) GDPR), "a cornerstone of data protection law",[870] which clarifies that all personal data must be

> "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes".

This principle, therefore, relates not primarily to the manner but to the reasons of the processing of personal data.[871] This principle is closely connected to the principle of proportionality as the legitimate aim for which data is processed is directly related to the proportionality assessment of the data processing. The European Data Protection Supervisor also emphasises the relationship between the principle of purpose limitation and the principle of proportionality, specifically "for public policies interfering with personal data protection, because the proportionality of the processing will have to be measured against the policy purpose selected by the legislator."[872]

The Police and Criminal Justice Authorities Directive contains the first part of this principle almost verbatim, but not the latter part concerning research and statistics (article 4 (1) (b) of the Directive). Instead, the Directive contains a second and third paragraph in article 4. According to these following paragraphs of the same provision, further processing is permitted under certain conditions:

869 Article 29 Working Party, Opinion 1/2013, p. 4 f.
870 EDPS Opinion 6/2015, p. 6. See also Korff (2014), p. 89.
871 Article 29 Working Party, Opinion 1/2014, p. 16. See also Korff (2014), p. 89; Simitis (1998), p. 2474; Durner (2006), p. 216 f.; Buchner (2016), p. 156 f.; Richter (2015), p. 736.
872 EDPS Opinion 1/2017, p. 8. See also Simitis (1998), p. 2478; Lynskey (2014), p. 594; Buchner (2016), p. 157.

> 2. "Processing by the same or another controller for any of the purposes set out in Article 1 (1) other than that for which the personal data are collected shall be permitted in so far as:
>
> (a) the controller is authorised to process such data for such a purpose in accordance with Union or Member State law; and
> (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.[873]
>
> 3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1 (1), subject to appropriate safeguards for the rights and freedoms of data subjects.
>
> 4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3."



The purposes of article 1 (1) of the Directive mentioned in this article are "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security." The European Data Protection Supervisor correctly criticises that there is no clearer definition of the principle of purpose limitation in the Directive. According to the EDPS, the prohibited incompatible further processing should have been properly defined in order to ensure that no lacunae develop.[874] Due to the nature of the data processed by the law enforcement sector, the principle of purpose limitation should have been given particular weight and protection in the system of the Directive.

The third principle is *the principle of data minimisation*.[875] According to article 5 (1) (c) GDPR, the collected personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". It should be emphasised that the principle of proportionality lies at the centre of this principle, demanding that data processing is limited to what is necessary.[876] The

873 See also EDPS Opinion 6/2015, p. 6. Footnote added by the author.
874 EDPS Opinion 6/2015, p. 6 f.
875 See in this context also Chapter VII below.
876 Article 29 Working Party, Opinion 1/2014, p. 13. See also Simitis (1998), p. 2478; Raabe/Wagner (2016), p. 436.

principle of data minimisation relates closely to the principle of purpose limitation, as the reasons for the processing of personal data naturally circumscribe how much data must be processed in order to achieve the purpose.[877] The wording used in the Police and Criminal Justice Authorities Directive is slightly different. Instead of the imperative "limited to what is necessary", the Directive uses the rather more open expression "not excessive" (art. 4 (1) (c) of the Directive).

The fourth principle is *the principle of data accuracy* (article 5 (1) (d) GDPR), according to which the data must be "accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". The wording used in the Police and Criminal Justice Authorities Directive is the same (article art. 4 (1) (d) of the Directive).

The fifth principle is *the principle of storage limitation*, set forth in article 5 (1) (e) GDPR. According to this provision, personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". This provision goes on to include an exception, however, according to which

> "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this regulation in order to safeguard the rights and freedoms of the data subject".

This rule, in combination with the case law concerning this principle, makes it abundantly clear that retention of data longer than necessary is incompatible with this principle and therefore unlawful.[878] The first element of this principle is included in the same way in the Police and Criminal Justice Authorities Directive, omitting the second element (article 4 (1) (e) of the Directive).

877 Article 29 Working Party, Opinion 1/2014, p. 16; Schantz (2016), p. 1841 f.; Bizer (2007a), p. 353.
878 Article 29 Working Party, Opinion 1/2014, p. 18.

The sixth and final principle is *the principle of integrity and confidentiality* (article 5 (1) (f) GDPR), according to which personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures". The same wording is used in the Police and Criminal Justice Authorities Directive (article 4 (1) (f) of the Directive).

Thus, all processing of personal data of European Union citizens must comply with at least these provisions and principles in order to be lawful. On top of those principles, there are of course also the general principles of, among others, proportionality and subsidiarity, which are applicable to all legislation of the European Union.



**viii. Rights of the Data Subject**

The principles of data protection are supported by a number of rights. These rights are necessary in order to enforce the application of the principles of data protection.[879]

In the first place, there is the *right to information* (article 13 and 14 GDPR). The data subject has the right to learn from the controller, among other things, the identity of the controller, contact details of a data protection officer, the purposes of processing, and the identity of recipients of personal data (article 13 (1) (a)-(f) GDPR).[880] Furthermore, the controller must inform the data subject at the time of collection of personal data of the period for which the data will be stored (if possible), of the other rights of the data subject, and of the existence of automated decision-making, if any.[881] A similar set of information must also be handed to the data subject if the controller has not collected the personal data in question from the data subject directly (article 14 GDPR).[882]

879 For notes on how the data subjects may be empowered by data protection legislation, see Blume (2012), p. 29 ff.
880 Boehm/De Hert (2012), p. 9; Bier (2015), p. 742 f.; Jaspers (2012), p. 572. See Salom (2014), p. 181.
881 See in this context also Wachter/Mittelstadt/Floridi (2017), p. 79 f.
882 Bier (2015), p. 742 f.

The Police and Criminal Justice Authorities Directive contains a similar right in Article 13 of that Directive. This provision gives the data subject the right to information concerning the identity and contact details of the controller and of the data protection officer, the purposes of processing, and the other rights of the data subject.[883] There is a second set of information which must be provided to the data subject in "specific cases", among other things concerning the legal basis on which data is processed, the retention period, recipients of this data, and "where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject" (article 13 (2) (d) of the Directive).[884] The third paragraph of article 13 of the Directive contains a rather wide exception, allowing Member States to delay, restrict, or omit to provide information pursuant to the previous two paragraphs.[885] This exception can apply whenever the Member State deems it necessary in order to avoid obstruction of inquiries, prejudice of any activity of the law enforcement agencies, or the protection of public or national security or the rights and freedoms of others. This provision is therefore designed in a very broad manner, potentially rendering the content of the right to information nearly meaningless.

In the second place, there is the *right of access*. This right is contained in article 15 of the GDPR: "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data". In addition to accessing the personal data itself, the data subject also has the right to learn a number of other items of information related to his or her personal data. This includes information concerning the purpose of processing, recipients to whom personal data has been or will be disclosed, information on the source of the data if the controller has not collected it directly from the data subject, the expected retention period and how this period is determined, the existence of the other rights of the data subject, including the right to erasure and rectification and the right to lodge a complaint with the supervisory authority, and finally, information on automated decision-making and profiling (article 15 (1) (a)-(h) GDPR).

This right is also contained in the Police and Criminal Justice Authorities Directive (article 14 of the Directive). In this Directive, the right is in the first instance

883 Kugelmann (2012), p. 582 f.
884 Boehm/De Hert (2012), p. 10.
885 Schwichtenberg (2016), p. 608.

designed in a very similar way as in the GDPR, with the difference that this right is subsequently severely limited by the provisions contained in article 15 (1) of the Directive.[886] That article states that

> "Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access of the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the national person concerned".[887]

The reasons for such a restriction of the right to access can be varied, from the interest in avoiding the obstruction of inquiries, investigations, or procedures, and avoiding to prejudice the prevention, detection, investigation, or prosecution of criminal offences or the execution of penalties to the need to protect public and national security and the rights and freedoms of others (article 15 (1) (a)-(e) of the Directive). As the Article 29 Working Party correctly points out, such broad exemptions are not in line with the concept of interpreting exceptions to fundamental rights restrictively.[888]



In the third place, there are *the rights to rectification or erasure of personal data and restriction of processing*. The *right to rectification* is contained in article 16 of the GDPR, according to which the data subject can demand that the controller corrects inaccurate personal information without undue delay. This also includes complementing incomplete data.

The *right to erasure* of personal data is contained in the following article 17 of the GDPR.[889] According to that article, the data subject may demand that personal data concerning him or her is deleted, if the personal data is no longer needed for the purposes for which it was originally collected or processed, or when processing of personal data was based on the consent of the data subject and this

886 Article 29 Working Party, Opinion 1/2013, p. 5.
887 EDPS Opinion 6/2015, p. 7.
888 Article 29 Working Party, Opinion 1/2013, p. 5.
889 This right is often also called 'the right to be forgotten' but the clearer term 'right to erasure' is preferred here. See in this context also Chapter VII (d) below. See also Jaspers (2012), p. 572 f.; Leutheusser-Schnarrenberger (2015), p. 586 f.

consent was withdrawn. Furthermore, the data subject may demand erasure when they object to automated processing or profiling, when data has been unlawfully processed, or when a legal obligation to erase personal data falls to the controller. This right can be restricted when processing is necessary for the exercise of the freedoms of expression, when the controller is under a legal obligation to retain data, for legitimate interests of public health or other for archiving purposes, and finally, when the data is necessary for use in legal proceedings (article 17 (3 (a)-(e) GDPR).[890]

The *right to restriction of processing* is found in article 18 of the GDPR, and can be applied in different situations. In the first place, processing of data can be restricted for the period of time while the controller verifies the accuracy of data. In the second place, processing can be restricted when the processing is unlawful but the data subject still prefers that data is not deleted. Finally, there may be situations in which the data has become unnecessary for the controller, but is needed by the data subject in a legal proceeding (article 18 (1) (a)-(d) GDPR).

These three rights are combined in article 16 of the Police and Criminal Justice Authorities Directive.[891] Paragraph one of that article provides for essentially the same right to rectification as article 16 of the GDPR does.[892] The second paragraph contains the right to erasure, particularly where processing infringes a principle of data protection, goes beyond what is necessary, or concerns sensitive data (article 16 (2) jo. articles 4, 8 and 10 of the Directive).[893] The third paragraph of article 16 concerns restriction of processing. According to this provision, the controller restricts processing when a decision on the accuracy of data is pending, or when personal data is retained as evidence (article 16 (3) (a) and (b) of the Directive). According to the following paragraph four, all those rights can, however, be limited in the same way as the other rights already discussed.

In the fourth place, there is the *right to data portability*, pursuant to article 20 GDPR. According to this provision, the data subject has the right to receive personal data in a format that makes it easy for another controller to use this data,

890 See on the conflict between freedom of expression and privacy Docksey (2016), p. 195 ff.
891 Schwichtenberg (2016), p. 608.
892 The only differences in language are caused by the fact that the GDPR as a regulation directly establishes the right to rectification, while the Police and Criminal Justice Authorities Directive places an obligation on Member States to establish this right in national law.
893 See also Article 29 Working Party, Opinion 14/2011, p. 26.

saving both the controller and the data subject time and energy.[894] The right to data portability is intended to make it easier for data subjects to switch from one service provider to another, allowing a service provider to utilise personal data collected by a predecessor. It is in the nature of this right that there is no equivalent to it in the Police and Criminal Justice Authorities Directive.

In the fifth place, the data subject has a *right to object* (article 21 GDPR). This right comes into play when data is processed pursuant an objective in the public interest, or pursuant the legitimate interests of the data controller or of a third party (article 6 (1) (e) or (f) GDPR). The data subject has the right to object to the processing of his or her data in those cases, based on the data subject's individual circumstances. This right is therefore very closely connected to the principle of proportionality. Again, the nature of this right is such that there is no equivalent right in the Police and Criminal Justice Authorities Directive.



In the sixth place, and related to the foregoing, is *the right not to be subjected to automated decision-making* (article 22 GDPR). "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" (article 22 GDPR).[895] There is no comparable right in the Police and Criminal Justice Authorities Directive. Instead, in article 11 (1), the Directive provides that

> "Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller."

There is therefore no right not to be subjected to automated decision-making in this context, but rather an obligation on Member States to draft the legal basis for such automated processing carefully. When special categories of data are the basis for such decision-making, this must not result in discrimination (article 11

894 Jaspers (2012), p. 573 f.
895 See in this context also Hildebrandt (2006), p. 550.

(3) of the Directive), and the processing must be subject to "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" (article 11 (2) of the Directive).[896]

Finally, there is the *right to lodge a complaint with a supervisory authority* and other remedies.[897] This right is found in article 77 of the GDPR, and is established just for the purpose stated in the name of this right, namely to ensure that "every data subject shall have the right to lodge a complaint with a supervisory authority" (article 77 GDPR). Furthermore, the following paragraphs regulate the right to an effective remedy against an offending controller or processor (article 79 GDPR)[898] as well as against the supervisory authority itself (article 78 GDPR). Finally, article 82 GDPR contains the right to compensation for material and immaterial damages suffered in consequence of an infringement of the terms of the GDPR.

The Police and Criminal Justice Authorities Directive also protects the right to refer a complaint to the supervisory authority in article 52 of the Directive.[899] The right to an effective judicial remedy against the controller or processor is enshrined in article 54 of the Directive, and the right to an effective remedy against the supervisory authority itself can be found in article 53 of the Directive. Finally, the Directive contains the right to compensation in article 56 for material and immaterial damages suffered in consequence of an infringement of the terms of the Police and Criminal Justice Authorities Directive.

All the rights contained in the GDPR can be restricted, pursuant to article 23 GDPR, "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society". The reasons for the restrictions are manifold. Among others, reasons to restrict the rights of the data subject are the need to protect public or national security, the interest in the prevention, investigation, detection, or prosecution of criminal offences and the enforcement of civil claims, the protection of judicial independence and proceedings, the protection of the data subject, and protection of the rights and freedoms of others (article 23 (1) (a)-(j) GDPR).

---

896 See also Article 29 Working Party, Opinion 14/2011, p. 19.
897 See also Article 29 Working Party Opinion 14/2011, p. 5.
898 See in this context also Göres (2005), p. 256.
899 See also the further discussion in Article 29 Working Party, Opinion 1/2013, p. 6; Kugelmann (2012), p. 583.

In contrast, the possibilities for restriction of the rights contained in the Police and Criminal Justice Authorities Directive are found in direct proximity to the right, either in the same article or in a following article. The formula chosen for restrictions in the Police and Criminal Justice Authorities Directive is similar as in the GDPR. It usually formulated in such a way that restrictions may be adopted, limiting "wholly or partly, the data subject's right […] to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard to the fundamental rights and legitimate interests of the natural person concerned". This particular formulation is that of article 15 (1) of the Directive, but the other provisions concerning limitations of the rights of the data subject are very similarly worded.

As can be seen, both the GDPR and the Police and Criminal Justice Authorities Directive contain a number of rights for the data subjects. While the rights contained in the GPDR are more extensive than those contained in the Directive, both instruments also contain a number of exceptions and derogations which may limit the application of those rights.



It should be emphasised once again in this context that as the rights of the data subject flow forth from the fundamental rights to privacy and data protection. Limitations to fundamental rights must always be interpreted narrowly.[900] It should be pointed out that this obligation to a narrow interpretation of limitations to fundamental rights applies to both the rights contained in the GDPR and also the rights contained in the Police and Criminal Justice Authorities Directive. Where limitations to a right are too wide, the underlying fundamental right is no longer properly respected, with the consequence of the legal norm being invalid.[901]

900 EDPS Opinion 6/2015, p. 7. See also European Commission (1999), p. 13; Kielmansegg Graf (2008), p. 23.

901 See the words of warning by *Giovanni Buttarelli* concerning the Police and Criminal Justice Authorities Directive, EDPS Opinion 6/2015, p. 7. See also Chapters IX and X of this thesis. For the interrelation of privacy, data protection, and surveillance, see Barnard-Wills (2013), p. 175 ff.

## e. Measures of Mass Surveillance

One of the main threats to an individual's privacy and private life is surveillance.[902] Surveillance will play a major role in the following chapters, particularly in Chapters IX and X,[903] and it should therefore be discussed in this context.

### i. Definitions

There is a great and increasing amount of literature on surveillance, with a great number of different definitions. The *Oxford English Dictionary* defines the term as "[w]atch or guard kept over a person, etc., esp. over a suspected person, a prisoner, or the like; often, spying, supervision; less commonly, supervision for the purpose of direction or control, superintendence."[904] In similar terms, "[s]urveillance refers to any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered".[905] This definition is generally applicable to all different types of surveillance. However, a distinction is generally made between targeted surveillance and mass surveillance.[906] Targeted surveillance in essence means the observation of a specific person or set of persons. Untargeted or mass surveillance on the other hand is essentially the observation of the behaviour of large groups or segments of the population.

Mass surveillance is increasing in application. This phenomenon has been observed and is viewed with concern by many commentators:

> "In the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection. As noted by the Special Rapporteur on the right to freedom of expression and opinion,

902 United Nations High Commissioner for Human Rights (2014), p. 3.
903 The first concern discussed in Chapter IX concerns the mass surveillance character of the measures of the anti-money laundering Directive. Chapter X asks the question, whether the principle of proportionality, which is now an essential test applied to assess the legality of an interference with the rights to privacy and data protection, is a suitable tool to address the cumulative effect of the growing number of measures of mass surveillance applied to the population.
904 Oxford English Dictionary, Third Edition 2010, s.v. "surveillance".
905 Dinev/Hart/Mullen (2008), p. 214.
906 Clarke (2015), p. 127. Clarke distinguishes between personal, location, and mass surveillance.

> technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. The State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before. In other words, the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it."[907]

There are different definitions for the term mass surveillance generated by and applied in the legal literature in the field. *Privacy International* supplies a useful definition in this context.



> "Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring. It involves a systematic interference with people's right to privacy. Any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance."[908]

For the purposes of this thesis, the concept of mass surveillance shall focus on the monitoring of behaviour of an undefined large group of people for the purposes of deterring, detecting or investigating undesirable, suspicious, or illegal behaviour. In addition, it must be emphasised that the notion of mass surveillance applied in this thesis is also connected to the absence of specific suspicions raised against the individuals to whom those measures are applied.[909]

Measures of mass surveillance occur with increasing frequency in the daily lives of all European Union citizens.[910] Examples of mass surveillance are the increasing web of video surveillance of public spaces,[911] the retention of communications

907 United Nations High Commissioner for Human Rights (2014), p. 3. See also Schmale/Tinnefeld (2017), p. 347.
908 Privacy international (no date). See also White (2013), p. 23 f.
909 Korff (2014), p. 115. See also Richter (2016a), p. 90.
910 Webster (2012), p. 22.
911 Lauritsen/Bøge (2012), p. 140 f.

data under the Data retention Directive[912] and the monitoring of an individual's financial transactions under the anti-money laundering regime.[913] All of those measures are applied across the board to all individuals who enter surveilled public spaces, who use publicly available electronic communications services, or who use financial services provided by any obliged entity under the Anti-money laundering Directive. The majority of the individuals to whom these surveillance measures are applied have not been suspected of any crime against which the measures are levelled, nor will the surveillance uncover any grounds of suspicion against them.[914]

**ii. Chilling Effects**

It can be observed that notions of surveillance are usually intimately connected to the action of observation, but not limited to it. Control and influence over the behaviour of the persons watched also plays a rather big role in the concept of surveillance.[915] For this reason, mass surveillance is usually intimately tied to the impact it has on individuals. The negative impact of surveillance on individuals is well documented:

> "Being watched can destroy a person's peace of mind, increase her self-consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities. We may want to protect against surveillance not merely to prevent disruptions of certain practices but to foster practices or to structure society in a particular way (by restricting the power of the government or employers)."[916]

It is clear that the average person does not behave quite in the same way in public as when he or she is alone in their home.[917] This corresponds to the observations already made in connection with the theory of spheres: Individuals will feel more comfortable in their private and intimate sphere particularly because they are not observed by strangers. In the same way, the impact of surveillance is dominated by the fact that an individual will behave differently when he or she knows that

912 Milaj/Kaiser (2017), p. 121 ff. See also Adamski (2012), p. 396 ff.
913 Milaj/Kaiser (2017), p. 123 f.
914 See also United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), p. 6.
915 Milaj-Weishaar (2017), p. 11 f. See also Schafer (2016), p. 593.
916 Solove (2002), p. 1130 f.; Harper (2012), p. 119 f.; Clarke (2015), p. 128. See in this context also Bentham (1791), p. 24 f.
917 See also the discussion of the Theory of Spheres in section (d) above in this Chapter.

someone is observing them.[918] If an individual must expect that they can be observed and that information on their conduct may be registered and processed, he or she may restrict him or herself, try not to be conspicuous,[919] and to escape the notice of the potential observer. This self-restraint is the chilling effect of surveillance. It is the reason for the fact that surveillance is also a powerful tool at the disposal of authoritarian regimes.[920] The strict control that can be exercised over a population by means of surveillance should be regarded as a serious danger to any free and democratic society.

Beyond the negative impact on the exercise of an individual's rights and freedoms, other concerns are raised against measures of mass surveillance. In the first place, criticisms concern the ineffectiveness of the measures in terms of a reduced crime rate or threat level,[921] and in the second place, it is argued that the principle of the presumption of innocence demands that persons not suspected of any crime should not be subjected to surveillance measures.[922]



In this context, it should be observed that not all commentators are entirely convinced of this negative character of measures of mass surveillance. For instance, *Hadjimatheou* argues that untargeted surveillance is less stigmatising and less intrusive than targeted surveillance.[923] This argument rests on the idea that for instance, if everyone must cope with security checks in airports, no specific person or group of persons will be singled out for security controls and therefore stigmatised by others. However, this argument disregards the fact that the group of persons which is targeted at airport security checks[924] would be defined around selectors of age, gender, and religion or ethnic origin. Such singling out would be incompatible with the right to non-discrimination and therefore inadmissible.[925] Furthermore, it is well-known that mass surveillance is often augmented by

918 Yngvesson (2012), p. 320 f.
919 Martini (2009), p. 841; Maras (2012), p. 74.
920 Mezzana/Krlic (2013), p. 8; Baum (2013), p. 583. See also Chapter X below.
921 Mezzana/Krlic (2013), p. 6.
922 Hadjimatheou (2014), p. 188. See also the sixth concern discussed in Chapter IX below.
923 Hadjimatheou (2014), p. 200 f.
924 See for a more detailed discussion Frowd (2012), p. 409 f. See also González/Bessa (2012), p. 295 f.
925 Naturally, such singling out and discrimination do happen. However, even the existence of such inadmissible discrimination cannot serve as a justification to introduce measures of mass surveillance: Mass surveillance does not prevent discriminatory targeted measures, it may in fact facilitate them. See for instance the discrimination in 'random selection' in airports, Frowd (2012), p. 409 f.

additional targeted surveillance, such as random selection in airport security checks, which may be based on profiling and has been linked to discrimination.[926]

Similarly, it is frequently argued that mass surveillance is at least not more intrusive than targeted surveillance, as mass surveillance measures generally interfere on a lower level with the rights to privacy and data protection of the data subject.[927] Furthermore, and in connection to the foregoing argument, it has been argued that the sweeping character of mass surveillance is irrelevant. It is contended that as the level of interference caused by mass surveillance is low and therefore the intrusion almost negligible, the interference does not achieve seriousness merely due to the fact that other individuals are under surveillance as well.[928]

Neither of these arguments can convince. The first argument is invalid because it ignores the practice of linking of information and the inferences that can be made based on data collected by mass surveillance. Therefore, even if the intrusions caused by mass surveillance were negligible, the amount of surveillance changes the situation. The simplicity with which information is linked leads to a situation in which information gathered through numerous surveillance measures may be combined easily. This would reveal a wealth of raw data about individuals, which may then be further enriched through data mining operations. This combination and augmentation of information may lead to exceptionally serious interferences with the rights to privacy and data protection of the individual.[929]

For instance, *Bull* mentions automatic registration of license plates on highways in this connection.[930] It is true that the individual datum that a certain car has been registered by a certain checkpoint at a certain time may in itself be of a low level of interference. However, a car will not be registered only once, but repeatedly over time and distances, which would allow for the establishment of a movement profile, the level of interference of which is undoubtedly rather high.[931] This is true particularly when this data is connected to other data collected by mass surveillance measures, such as that individual's mobile phone's location data collected under

926 Frowd (2012), p. 409 f. See also González/Bessa (2012), p. 295 f.
927 Bull (2006), p. 1620.
928 Bull (2006), p. 1620.
929 See also Chapter X below.
930 See in this context also Pocs (2011), p. 163.
931 See Hensel (2009), p. 528 f.

the data retention legislation[932] and that individual's financial transaction history collected under the Anti-money laundering Directive.

The second argument according to which the mass character of surveillance is irrelevant is therefore also invalid. Not only is the level of interference of mass surveillance in the times of integrated and interconnected databases[933] always potentially high and serious. In addition, the remarks made above on the potential societal costs of mass surveillance in terms of individual freedom and a free and democratic society should be considered in this context, which also serve to press the point that indeed it does make a difference whether the rest of society is under surveillance alongside oneself.

The most striking argument that can be raised against surveillance measures is, however, their potential intrusion into aspects of the private and intimate spheres of an individual's personality.[934] The high level of interference potentially caused by measures of mass surveillance also creates the danger that the interference reaches into particularly protected aspects of a data subject's rights. This concerns in particular the right to privacy with the special protection of an individual's intimate sphere as well as, to a somewhat lesser extent,[935] the protection of a data subject's sensitive data. It is therefore generally accepted that where surveillance measures are liable to intrude upon an individual's intimate sphere, strict safeguards must be put into place,[936] if indeed the interference may take place at all.[937]

> "A legal basis for a surveillance measure, which may affect the core values of an individual's privacy,[938] must ensure to the greatest possible extent



932 It should be noted that while the Data retention Directive was invalidated, some Member States may still or again enforce data retention legislation.

933 See also Waterman/Bruening (2014), p. 90 ff.

934 See in this context also the first concern discussed in Chapter IX below.

935 It has been shown above that the individual's intimate sphere is strictly protected, while the protection of a data subject's sensitive data is subject to a number of exceptions. However, the protection of the former has been developed in a long series of case law particularly by the BVerfG, while the protection of the latter is supplemented by significantly less case law. The CJEU does appear to assign much importance to the protection of sensitive data: see below the discussion of CJEU Opinion 1/15 *PNR* [2017].

936 Poscher (2009), p. 272.

937 See the remarks made on the connection between privacy and human dignity in this chapter above.

938 The BVerfG uses the term "Kernbereich privater Lebensgestaltung", which is very difficult to translate, but in the context of this thesis the term "core values of an individual's privacy" was chosen. See also Chapter X below. Footnote added by the author.

> that data relating to these core values are not collected. If, such as in the case of secret access to a computer system, it is practically unavoidable to take note of information before being able to evaluate whether this data relates to these core values, a sufficient level of protection must be ensured for the evaluation phase. In particular, discovered and collected data with such a relation to the core values must be excluded from processing and deleted without delay […].[939]

The BVerfG therefore demands that in the first place, data relating to a person's intimate sphere should not be collected in the first place wherever possible. If it is impossible to avoid the collection of such data, it must be deleted as soon as this relation is discovered.[940] This is also and especially true in the case of measures of mass surveillance introduced in order to be used in the fight against serious crime and terrorism. Whereas the current approach chosen by the lawmaker appears to be to assign paramount importance to the policy goal of curbing serious crime and especially terrorism, this policy choice cannot cause any reduction of the inviolability of human dignity.[941] While the lawmaker rather frequently appears to lose sight of this fact, and while especially the protection of the rights to privacy and data protection is at this point largely left up to the Courts,[942] it must be acknowledged that the Courts appear to be unafraid of asserting the importance of these rights.[943]

As a final point in this section, it should be emphasised that the legal framework in place to govern mass surveillance is entirely inadequate.[944] It is striking that the data protection framework currently in place is not addressing mass surveillance properly. The GDPR, for instance, was only passed in 2016, at a time when mass surveillance is applied at an increasing rate, and simultaneously public discourse concerning such measures is intensifying. Meaningful safeguards against mass surveillance are prominently absent from both the GDPR as well as from the Police and Criminal Justice Authorities Directive.[945]

939 BVerfG 1 BvR 370/07 [2008], paragraph 277.
940 Poscher (2009), p. 273.
941 Poscher (2009), p. 276.
942 See also Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 342.
943 See for instance CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 51; ECtHR Case of *Roman Zakharov v. Russia* [2015]. See also Skouris (2016), p. 1364; Tridimas (1999), p. 77; Solove (2007), p. 411; Waldron (2003), p. 191 f.
944 Koops (2014), p. 256 ff. See also Roßnagel (2016), p. 565; Baum (2011), p. 596.
945 Cannataci (2013), p. 24 ff.

## f. Conclusion

In the words of *Schoeman*, "Privacy as a topic is as fascinating as it is important."[946] The same is certainly true for the right to data protection, which has received more intensive public attention only after *Schoeman* made his above observation. As has been seen, two connected rights are thus protected by article 8 of the ECHR, and articles 7 and 8 of the Charter, namely the right to privacy on the one hand, and the right to data protection on the other hand.

These two rights are a particularly important set of rights for the population. This special importance of these two human rights lies in the first place in their close connection to the right to human dignity.[947] In the second place, privacy and data protection are two of the supporting pillars of a free and democratic society. Without the rights to privacy and data protection, freedom and democracy are simply not possible.[948] Therefore, the rights to privacy and data protection should also enjoy increased protection.



The most important points made in this chapter, which will play a major role in the third part of this thesis have all been discussed particularly in sections (d) and (e) of this chapter. The first major take-away from this chapter concerns the right to privacy. There are several points made in this Chapter V which will be of great importance in the following chapters: In the first place, the right to privacy and the notion of private and family life lie at the centre of particularly the following Chapters VIII, IX, and X. These chapters will expand on the proportionality of limitations of the rights to privacy and data protection in general (Chapter VIII), and on the proportionality of the interferences with the rights to privacy and data protection by the Anti-money laundering Directive in particular. The notion of privacy and the protection of personal data will play a major role in those chapters. Chapter X concerns especially the right to privacy and the essence thereof. This chapter will build on the remarks made in the present Chapter V particularly regarding the close connection between the right to privacy and human dignity.

946 Schoeman (1984a), p. 1.
947 Gurlit (2010), p. 1036; Bloustein (1984), p. 186 f.; Solove (2002), p. 1116; Lynskey (2014), p. 572.
948 Böhme-Neßler makes this argument very convincingly in Böhme-Neßler (2016), p. 5 f. See also De Hert (2003), p. 48; Tinnefeld (2007), p. 628; Maras (2012), p. 72.

Secondly, the discussion of the right to data protection is of importance for the analytical part of this thesis. This concerns in particular the concept of personal data, as this concept is the basis for all the discussion of data protection taking place in this thesis. Sensitive data and financial data could furthermore be considered to be two interconnected sub-categories of personal data. These two sub-categories will play a major role in each of the following chapters.

Personal data is, as will be seen, closely connected to an individual's identity: the whole concept of personal data rests on the identified or identifiable person. Similarly, sensitive data is also often closely related to the identity of the data subject. This connection will come into play in the following Chapters VI and VII. Furthermore, one of the cases discussed in Chapter VIII is the CJEU's opinion on the PNR agreement, in which the proper protection of sensitive data is highlighted. The lack of robust safeguards for sensitive data is furthermore the subject of the fifth concern discussed with respect to the Anti-money laundering Directive in Chapter IX; it is one of the pivots of the proportionality assessment conducted in that chapter. Similarly, the principles of data protection will play a role in those concerns, influencing the discussions of six[949] out of the seventeen concerns mentioned in Chapter IX. The rights of the data subject will also be brought into the discussion of the Anti-money laundering Directive, particularly the right to information in the tenth concern.

Lastly, the concept of (mass) surveillance will play a major role in Chapters IX and X. In Chapter IX, it is one of the most important concerns to be discussed with respect to the proportionality of the Anti-money laundering Directive. The first concern to be discussed in Chapter IX is dedicated to the mass surveillance character of the anti-money laundering measures. All of the remarks made in section (e) of this Chapter V are also going to come into play, and going to be further expanded and developed, in Chapter X of this thesis.

949 Namely particularly the third, tenth, eleventh, thirteenth, fourteenth, and sixteenth concerns.

# Chapter VI

## Identity and Identification

## Outline:

a. Introduction
b. Identity and Identification
    i. Definition
    ii. Social and Personal Identity of an Individual
    iii. Identification
    iv. Social Identity and the State
c. Identity and Identification in Data Protection Legislation
    i. Identity and Personal Data
    ii. The Identified or Identifiable Person
    iii. Full, Partial and Functional Identity
    iv. Direct and Indirect Identification
d. The Protection of Identity
e. Privacy and Identity in Financial Transactions
    i. The Conventional Banking Sector
    ii. Virtual Currencies
    iii. Informal Value Transfer Systems
f. Conclusion

## a. Introduction

The concept of Identity is closely connected to that of personal data.[950] As has already been shown, personal data relates necessarily to an identified or identifiable person, and is not protected by data protection legislation in the absence of such a link. Therefore, the concept of identity is a particularly important concept in data protection law.[951] In addition, the concept of identity and identification of a person has been mentioned several times already in connection with the European anti-money laundering legislation. All obliged entities are required to make sure that all customers are identified as soon as anti-money laundering measures become applicable.

Particularly in sociology and in law, the term identity is not yet pinned down to one uniform definition. *James Fearon* lists 14 different definitions of the term identity in related disciplines.[952] Various different concepts of identity have been constructed and developed by different authors over the years. However, many theories are only used to discuss certain sociological aspects of the wide field that is identity, and thus cannot be applied to the very specific subject matter of this research. Therefore, this thesis will limit itself to discussing the concepts of social and personal identity, following the work of, among others, *James D. Fearon* and *Richard Jenkins*.[953] After a discussion of the meaning of these two concepts, they will be applied to the users of virtual currencies and of informal value transfer systems. The application of the concept of personal identity allows extra light to be shed on the reasons why people may prefer one of the alternative financial transaction systems over the conventional banking system, and in a second step, the concept of social identity can help explain how a person's choice for a certain transaction system can influence the view other persons take of him or her. This second concept will thus also play a role in later chapters of this thesis, and can help understanding the views of the public, reactions of policy makers, and actions taken by law enforcement agencies, as they are based to some extent on the social identity of the users of a given transaction system.



950 Lynskey (2014), p. 590; Hohmann-Dennhardt (2006), p. 546; Schmale/Tinnefeld (2010), p. 527 f.
951 Korff (2014), p. 88. See also the submissions of the Austrian Government in CJEU Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003], paragraph 52. See also Ballard (2013), p. 107; Deighton (2003), p. 138.
952 Fearon (1999), p. 4.
953 Jenkins (2008), p. 17; Fearon (1999), p. 2.

This chapter is intended to give a closer look into the concept of identity, both from a selected social sciences perspective as well as from a legal perspective. The findings presented in this chapter are going to be of great value as background to the obligation to identify customers under the Anti-money laundering Directive, and to the interference this identification causes with the customer's rights to privacy and data protection. In addition, the observations on the meaning of the term identity will help rounding off the theoretical framework within which the anti-money laundering legislation is going to be evaluated.

This chapter follows a ternary organisation in order to shed light on all aspects of the concept of identity. After the introduction, a discussion of identity as a personal and social concept is introduced (b), which is followed by a discussion of the concept of identity as it is understood in legal terms, particularly within the data protection framework (c). A brief discussion of the protection of identity in the data protection and privacy framework follows (d). Finally, those concepts of identity are to be translated to the system of financial transactions, to discover how a person's social and personal identity play a role in an individual's choice for and use of a certain transaction system, and the application of identification regimes to the users of those transactions systems (e).

## b. Identity and Identification

### i. Definition

The word *identity* has a host of different definitions in different contexts.[954] Although virtually everyone has an understanding of the meaning of the concept of identity, this term means vastly different things to different people and in different disciplines of science. There is not one universally accepted definition, and vastly different concepts can be associated with the notion, depending on the angle from which one looks at the term identity.[955] *Brubaker and Cooper* understandably lament that the term "tends to mean too much (when understood in a strong sense), too little (when understood in a weak sense), or nothing at all (because of its sheer ambiguity)."[956] In a similar vein, *Jenkins* comments that "Much writing

954 Schröder/Morgner (2013), p. 532.
955 See also Roosendaal (2013), p. 18 ff.
956 Brubaker/Cooper (2000), p. 1. See also Schröder/Morgner (2013), p. 532.

about identity treats it as something that simply is", without properly discussing the precise concept they understand this term to convey.[957] *Diderot and d'Alembert* make this point rather comically clear in their definition of the term identity:

> *"Une chose considérée en divers lieux; ou en divers tems, se retrouvant ce qu'elle étoit, est alors dite la même chose. Si vous la considériez sans nulle différence de tems ni de lieu, vous la diriez simplement une chose; car par rapport au même tems & au même lieu, on dit voilà une chose, & non voilà la même chose."*[958]

The term 'identity' is derived from the Latin word idem, meaning "the same", and has been used in the English language since at least the 16th Century.[959] The definition of the term is disputed, and different approaches can be found in each discipline. For common usage of the term, we turn to a dictionary of the English language. The Oxford English Dictionary lists several definitions for identity, in different contexts. The first and main definition relates to things: "The quality or condition of being the same in substance, composition, nature, properties, or in particular qualities under consideration; absolute or essential sameness; oneness",[960] and the second instance refers to people, stating "The sameness of a person or thing at all times or in all circumstances; the condition of being a single individual; the fact that a person or thing is itself and not something else; individuality, personality."[961] This assessment also coincides with the observations made by *David Hume*:

> "The same reasoning extends to identity. We readily suppose an object may continue individually the same, though several times absent from and present to the senses; and ascribe to it an identity, notwithstanding the interruption of the perception, whenever we conclude, that if we had kept our eye or hand constantly upon it, it would have conveyed an invariable and uninterrupted perception. But this conclusion beyond the impressions of our senses can be founded only on the connexion of cause and effect; nor can we otherwise have any security, that the object is not

957 Jenkins (2008), p. 17. See also Deighton (2003), p. 138 f.
958 Diderot/d'Alembert (2016) s.v. "Identité"
959 Gleason (1983), p. 911.
960 Oxford English Dictionary, Third Edition 2010, s.v. "Identity".
961 Oxford English Dictionary, Third Edition 2010, s.v. "Identity".

> changed upon us, however much the new object may resemble that which was formerly present to the senses."[962]

In rather informal terms, it could also be stated that a person's identity is expressed by that person in answer to the question "who are you?"[963] To a lesser extent and in order to detach the definition of a person's identity from his name alone, persons can also be asked, "what are you?" Thus a person's identity is in the first place that person's own idea and definition of him- or herself. This approach to a person's identity seems to be the most basic and universal, the meaning most persons associate with the term 'identity'.

In Philosophy, it has been discussed extensively and in depth what an identity really is. The discussion evolves around the question which particular attributes, properties or qualities of a person or a thing make up the set of necessary values according to which a person or a thing is that particular person or thing.[964] If these essential features were to be changed, the person or thing in question would lose its former definition and be someone or something else. *Fearon* cites several questions that may arise in that connection in order to illustrate the problem:

> "What makes that tree the same tree that was there 20 years ago? If you rebuild a boat plank by plank, does it remain the same boat? Or, in terms of persons, what would have to be different about me for me to no longer be who I am? What are the properties or qualities in virtue of which I am James Fearon?"[965]

Personal Identity in this context is thus the sum of "*essential*" instead of "merely *contingent*" attributes and characteristics of a person.[966] If only one of these attributes is changed, the entire person is no longer the same as it was before.[967] To illustrate this, *Fearon* states that in this way, losing a limb does not necessarily

962 Hume (1740), Book I, Part III, Section II, 'Of Probability, and of the Idea of Cause and Effect'. See also Ballard (2013), p. 129.
963 Fearon (1999), p. 11; Mead (1934), p. 200; See also De Hert (2003), p. 85.
964 Fearon (1999), p. 12. See also Murphy (1984), p. 42 f.
965 Fearon (1999), p. 12. These are essentially the examples already cited in 1765 by Diderot/d'Alembert (2016) s.v. "Identité". See also Hume (1740), Book I, Part I, Section V, 'Of Relations'.
966 Fearon (1999), p. 12. Emphasis retained from the original.
967 Fearon (1999), p. 12.

change the identity of a person, but suffering from a severe mental illness may cause others to regard a person as different than before.[968]

Indeed, the foregoing already illustrates the problem with the definition of an identity of a person very aptly. *Hume* brings this problem to the point when he observes:

> "It is certain there is no question in philosophy more abstruse than that concerning identity, and the nature of the uniting principle, which constitutes a person. So far from being able by our senses merely to determine this question, we must have recourse to the most profound metaphysics to give a satisfactory answer to it; and in common life it is evident these ideas of self and person are never very fixed nor determinate."[969]

Very simply put, across all sciences, it can be said that "Identity is our understanding of who we are and who other people are, and, reciprocally, other people's understanding of themselves and of others (which includes us)."[970] This concept coincides with the dictionary definition cited above. Taking this concept as a starting point, the notion of identity has been developed, particularly in recent years, in many different disciplines, and has received a host of different connotations in sociology, psychology, history, and law.



**ii. Social and Personal Identity of an Individual**

Thus, it can be distinguished between a social identity and a personal identity. In the first place, a person's social identity refers to the placement of that person in a certain social group, category, or segment of the population,[971] "a set of persons marked by a label and distinguished by rules deciding membership and (alleged) characteristic features or attributes."[972] Those social categories can be created by the members themselves, or created by society to place them into. These groups will have a common predicate, such as physical appearance, ethnic background, sexual preference, or any other attributes, and society attaches certain expectations

968 Fearon (1999), p. 12.
969 Hume (1740), Book I, Part IV, Section II, 'Of Scepticism with Regard to the Senses'.
970 Jenkins (2008), p. 18.
971 Fearon (1999), p. 2, 13.
972 Fearon (1999), p. 2, 13 f. See, in this context, also Schwartz (1968), p. 741; Murphy (1984), p. 42 f.

and prejudices to members of these groups, simply because of their (alleged) membership in it.[973]

An individual's personal identity, on the other hand, includes one or more certain characteristics, beliefs, visions or principles, or attributes, that a person considers to be particularly expressive of him- or herself.[974] It is basically those features which a person considers particularly important or unique to him- or herself, and which are different from the features observed in other individuals.[975]

According to *Fearon*, this feature might anchor a person's identity for different reasons. In the first place, it might be something that the person is especially proud of or considers especially defining for him- or herself, for example a person's outward appearance, heritage or education.[976] In the second place, it might be a decisive guide for this person's actions, such as the person's religious beliefs, philosophy, or certain cultural norms.[977] Lastly, this might be a set of attributes that a person is so attached to, that he feels that he or she cannot be separated from them and their influence on his or her behaviour.[978] Particularly this second category is highly subjective, and may comprise attributes from any other above mentioned group of attributes.

The distinction between social and personal identity in social sciences is useful for a brief discussion of the term 'identity' as intended here, but it is by no means undisputed. *Jenkins*, for example, argues that the emphasis on the 'social' aspect is redundant, as identity is always social, considering that also personal identity largely depends on how an individual distinguishes himself from the rest of society.[979]

### iii. Identification

Identification is, based on the observations made on the concept of identity above and very simply put, the act of establishing one's own or someone else's identity.[980]

973 Fearon (1999), p. 2.
974 Fearon (1999), p. 2; Schwartz (1968), p. 747; Maras (2012), p. 74. See in this context also the discussion of sensitive data above in Chapter V (d).
975 Fearon (1999), p. 21 f.; Mead (1934), p. 200 f.
976 Fearon (1999), p. 11. See also Nicoll (2003), p. 99.
977 Fearon (1999), p. 11
978 Fearon (1999), p. 11.
979 Jenkins (2008), p. 17. See also Mead (1934), p. 200 f.
980 Oxford English Dictionary, Third Edition 2010, s.v. "Identify".

One may also define this concept as "every act that infringes upon a person's anonymity and through which a person loses the privilege of not being held to the full rules of role expectations that would operate if he/she were known to those observing him/her."[981] This second definition ties a person's social and personal identities directly to one another. Identification can occur with or without a person's knowledge, and can be carried out by both the individual and another person or by way of an automatic process.

*Jenkins* attempts to define identification in the discipline of sociology with a three-tier structure. In the first place, "identity denotes the ways in which individuals and collectivities are distinguished in their relations with other individuals and collectivities".[982] The word collectivities here means groups of individuals. Secondly, "Identification is the systematic establishment and signification, between collectivities, and between individuals and collectivities, of relationships of similarity and difference",[983] and finally, "taken – as they only can be – together, similarity and difference are the dynamic principles of identification, and are at the heart of the human world".[984]



This definition requires some clarification. According to *Jenkins*' model, each person possesses a set of dynamic attributes. Those attributes can be of any order. A person's visible attributes are important, such as that person's age, gender, and ethnic origin, but also attributes that are often not as easily discernible from the outside, such as a person's income level, education, and sexual orientation. However, the set of these attributes comprises an individual's identity. They determine the way this person sees him- or herself, and the way others see that person.

The individual is placed into groups of people sharing a particular attribute. That way, this person can be young, which is an attribute shared by other young people, but not by the group of elderly people. The person could be female, and share this attribute with roughly half the population, but most of the other half of the population would have the attribute male instead. Furthermore, the person in

981 De Hert (2003), p. 47 f. See in this context also the observations made on privacy and human dignity above in Chapter V (d), as well as on surveillance in section (e) of that Chapter.
982 Jenkins (2008), p. 18.
983 Jenkins (2008), p. 18. See in this context also Lioy (1891), p. 33 ff.
984 Jenkins (2008), p. 18. See in this context also Simmel (1906), p. 451.

question might be Muslim, and share that attribute with the other members of the Muslim community, but not with the persons of other faiths or atheists.

The attributes a person sees in him- or herself determine to which group of people they feel they belong (based on similarities) or do not belong (based on differences). But these attributes are also read and interpreted by other individuals, and a person is placed into groups by those individuals based on the perception of similarities and differences of that person to other persons in society.[985] This process of responding to similarities and differences between people is what is meant by identification by Jenkins in this context. Needless to say, these perceptions can often be wrong, especially because at this stage, prejudices, emotions, and subjective experiences come into play.

Prejudices are applied where society perceives a person's social identity and applies generalizations to that person.[986] Generalizations can be made about almost any social category of persons,

> "in terms of sets of characteristics – for example, beliefs, desires, moral commitments, or physical attributes – thought typical of members of the category, or behaviours expected or obliged of members in certain situations, as in the case of roles, such as a professor, student, or police officer."[987]

This application of generalizations can be useful, for example when applied to a group of persons in the same profession, which allows people then to gauge the social situation when in contact with, for instance, a police officer. Generalization does present a problem, however, when generalization of social groups of persons, such as religious and ethnic minorities, are negatively constructed, and lead to discrimination, stigmatization,[988] and racism.[989]

985 See also Mead (1934), p. 200 f.
986 Fearon (1999), p. 2.
987 Fearon (1999), p. 14. See also Maras (2012), p. 75.
988 See for background on stigma fundamentally Goffman (1963).
989 See also Maras (2012), p. 73.

**iv. Social Identity and the State**

Discrimination is a rather important topic whenever the data subject comes into contact with the state, particularly with law enforcement agencies. The fact that the state must necessarily always be represented by natural persons means that this representative of the state very likely carries concepts of social identity within him.[990] If a person belongs to a group of persons with which other groups of society connect negative associations, such as is sadly often the case for ethnic and religious minorities, the representative of the state may not be free of those negative prejudices either. There is thus an increased danger that a person's social identity can have negative consequences for him or her if they come into contact with the state authorities.[991]

The drafters of the legal framework have evidently recognized this danger and, as will be explained in further detail in the following section of this chapter, the data protection legislation therefore also makes a clear reference to the cultural and social identity of a person in the data protection framework. According to the oft-quoted article 4 (1) of the GDPR,

> "'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".

The possible grave negative consequences which can be attached to a person's perceived membership in a certain group makes it imperative to protect certain categories of personal data as especially sensitive, and to avoid references to those categories as much as possible. However, the system is imperfect, as a person's first and/or last name will often give away his or her ethnic origin, and a passport picture of a woman with a headscarf is a clear reference to her religion.[992]

990 See in this context also Arendt (1973), p. 185 ff.
991 Hadjimatheou (2014), p. 198. See also Ferret (2012), p. 325.
992 This observation is also pertinent to the discussion of the revelatory character of financial data later in this chapter and in Chapters V (d) and IX.

The connection between a person's social identity and the general judgments the rest of society attaches to a person's membership in a certain group acts as the explosive agent in this context. Some prejudices have proven themselves to be almost ineradicable in the greater social context, and it can hardly be expected that all members of a society will abandon the convenient concept of a society partitioned into many different social groups, however desirable such desistance may be. Applying the same judgments, expectations, and stereotypes to all members of a certain social group very much simplifies a complex society, and is therefore attractive to many people.

However, this behaviour is naturally inacceptable particularly when shown by persons representing the state, such as the police or the judicial apparatus.[993] Especially when the membership of an individual in a certain group or class is connected to prejudices concerning crime,[994] the absence of such prejudices in persons representing the state becomes imperative. As *Dworkin* very fittingly puts it, "it is unjust to put someone in jail on the basis of a judgment about a class, however accurate, because that denies his claim to equal respect as an individual."[995] Of course, the imprisonment of a person solely because of their (perceived) membership in a certain group is an extreme example. But surely any negative attitude towards a person solely based on their membership in such a group is inacceptable.[996] The importance of this connection to the very basic concepts of human rights can hardly be overstated. Unmerited negative judgments made by anyone can be hurtful to individuals as well as, naturally, to society as a whole, but are nothing compared to the potential seriousness of the consequences of unmerited negative judgments made by representatives of the state, which can have very real legal implications for individuals.[997]

993 See also Hadjimatheou (2014), p. 198.
994 See in this context the discussion of the link between Hawala and terrorist financing in Chapter III above.
995 Dworkin (1977), p. 13.
996 See for the connection to human dignity Bou-Habib (2008), p. 162.
997 See the remarks made on discrimination in section (e) of Chapter V above and in Chapter IX below.

## c. Identity and Identification in Data Protection Legislation

### i. Identity and Personal Data

Social sciences are not the only branch of sciences in which much time and energy has been invested into the research of the concept of identity. The concept of identity is different than that applied in social sciences, but it is to some extent shaped by and builds upon the discussions outlined in the previous sections.

The concept of identity in law also has a long historical tradition, considering the importance of establishing the identity of victims and offenders in criminal law, or the establishment of the identity of a passport-holder at national borders. The comparatively recent legislation on data protection and privacy has also had a big impact on the legal concept of identity. This is due to the central position this term is taking in the data protection legislation, which defines protected personal data as "information relating to an identified or identifiable natural person" (article 4 (1) GDPR). This central position of this term has naturally led to further development of this concept in both case law and literature, some of which has already been referenced in the previous Chapter V.



A clear difference between sociological literature and legal literature on the concept of identity is that in sociology, identity and identification is subjective, in the sense of personal preference and how a person is perceived or perceives himself, while in legal science, identity is neither primarily personal nor social; the subjective preferences of the individual are moved into the background. What is important in the legal concept of identity and identification is how one natural person can be clearly distinguished, in objective terms, from the rest of the population.[998]

In many countries, this is simply achieved by a unique citizen identification number assigned to each person.[999] Such a citizen identification number is often directly connected to a database collecting a number of references to a person's identity. Most commonly, those are the full name and any previous names if the person has ever undergone a name-change, date and place of birth (and, later on, death). Further stored information may include the individual's gender, address, a

998 See also Meints/Hansen (2006), p. 561 f.
999 Prominently in the Netherlands in the *Wet algemene bepalingen burgerservicenummer* of 2007. See also Vandezande (2011), p. 11 f.

facsimile of his signature, a biometric facial photograph, and fingerprints.[1000] All of those identifiers are objectively determined attributes about an individual.

However, in some areas of law, the concept of identity is undergoing a change. A person's identity no longer relies solely on those objective markers, but other factors can come into play.[1001] The prominent case for this development is the European data protection legislation. This legislation does not only indirectly protect a person's identity by protecting information relating to an identified or identifiable person, but rather goes further than that. The definition of personal data in article 4 (1) of Regulation 2016/679 particularly mentions "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Although it is laudable that the regulation also contains more subjective and intangible concepts of identity, such as a person's cultural and social identity, none of those terms are properly defined and therefore very difficult to apply.

Furthermore, some elements of a person's identity are considered to merit especial protection.[1002] The categories of sensitive personal data in article 9 (1) of the GDPR have already been discussed in the previous chapter. This provision reads,

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

It should be noted that all of those elements have a clear relationship with a person's social and/or personal identity, particularly a person's racial or ethnic origin, religion, and sexual orientation, which may be very important for an individual's personal identity, but are at the same time especially notorious for attracting negative prejudices when they flow into a person's social identity.

1000 See Sullivan (2011), p. 21 f.
1001 See also Schmale/Tinnefeld (2010), p. 527 f.
1002 See CJEU Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003], paragraph 52. See also Lynskey (2014), p. 590.

The European data protection legislation thus acknowledges that a person's identity is more than just a name, address and date and place of birth. Yet, this apparent extension of the term identity does not invalidate what was stated above: The main notion connected to the identity of a person concentrates on distinguishing individuals from one another. Even in the context of data protection and privacy legislation, in the foreground is always the question whether or not a person can be clearly distinguished from the rest of the population.

**ii. The Identified or Identifiable Person**

It has already been emphasised that the 'identified or identifiable person' is a central term in the GDPR. The Article 29 Working Party defines this term as follows: "In general terms, a natural person can be considered as 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group."[1003] This coincides with the dictionary definition of identity in law already given at the beginning of this chapter. The term identifiable, in this context, means that the identification of a person has not yet taken place, but he or she could be identified.[1004]



A person is normally identified by the combination of so-called 'identifiers'.[1005] Identifiers are "particular pieces of information […] which hold a particularly privileged and close relationship with the individual."[1006] Many different kinds of information can serve as identifiers. The most common identifiers are name and date of birth, as was already mentioned above, but also information on an individual's personal appearance, such as height, eye colour, or even biometric data can be used.[1007] Other information may even pertain to a person's profession, hobbies, and daily habits.

This same logic is also applicable in an electronic context. In a small sample, one characteristic can be enough to identify a person, while in a larger sample, say, the population of a country, a combination of a number of these identifying attributes can individually identify each person. The more identifiers are used to identify a person, the more accurate the identification becomes; the chance of the sample containing a second person sharing the same attributes becomes smaller. For

1003 Article 29 Working Party, opinion 4/2007, p. 12.
1004 Article 29 Working Party, opinion 4/2007, p. 12.
1005 See also Hammer/Knopp (2015), p. 504.
1006 Article 29 Working Party, opinion 4/2007, p. 12.
1007 De Andrade et al. (2014), p. 5. See also Monteleone (2012), p. 5 f.; Pocs (2011), p. 164 f.

example, although identical twins may share the same physical appearance, they will have different names; although a parent and a child may have the same name and address, their birthdates will be different; although two persons with the same name may be born in the same city on the same date, their physical appearances will be different. Thus, even in a large group of people, if one continues to add identifiers, eventually only one individual will be left to whom all of the identifiers apply. This person is then identified.

### iii. Full, Partial, and Functional Identity

*De Andrade et al.* make a useful distinction in this context between a person's full identity, a person's partial identity, and a person's functional identity.[1008] Under this distinction, a person's full identity consists of the sum of all collected identifiers pertaining to that person. A typical European identity card for example may list a person's full name and possible pseudonyms, date and place of birth, sex, nationality, and address, along with certain physical characteristics, such as height and eye colour, a biometric picture, and the person's handwritten signature.[1009] Furthermore, Identity cards can contain electronic information including a person's fingerprints, iris scans and other electronic identifiers.[1010] The sum of the available identifiers, uniquely identifying a person, makes up a person's full identity.

On the other hand, a person's partial identity only refers to his answering to a certain identifier.[1011] It can be imagined that there are instances when a person's name or address is of no consequence, but only his age, for example when a customer wishes to buy alcohol or cigarettes, which may be only available to persons over the age of 18. Which identifiers a person's partial identity encompasses usually depends on the purpose of the identification. For example, as an ID card is a document used for multiple different purposes, it contains many different general identifiers. A driver's license, in contrast, will list among other information a person's full name and date and place of birth, and the different vehicles which the person is allowed to control on public roads, but it may not contain the person's address or

1008 De Andrade et al. (2014), p. 5. See also Nabeth (2006), p. 541 f. This distinction will come into play for instance in the following Chapter VII (d).
1009 The German identity card was used for a reference in this case.
1010 This information is also often contained in passports.
1011 De Andrade et al. (2014), p. 5.

nationality, since these particular pieces of information have no influence on a person's driving.[1012]

Lastly, a person's functional identity lies inbetween the concepts of full and partial identity. A person's functional identity is generated by adding identifiers until there is only one person to whom all those identifiers apply: the identifiers used to establish the person's identity "are 'the same' as the attributes of that person and therefore serve to identify that exact person, since they are not the same as – that is, not identical to – the combined attributes of any other person".[1013] The information needed in each individual case therefore depend largely on the sample in question. Identification may be achieved by using only one identifier if it is unique enough, like a citizen identification number[1014] or a biometric picture,[1015] or by a more simple identifier such as the person's full name in a smaller sample. The functional identity of a person is less than a full identity, because further available identifiers are not needed as soon as one individual is singled out.[1016] On the other hand, a functional identity goes beyond a person's partial identity because identifiers typically used to establish a person's partial identity can apply to a large group of persons.



The application of partial and functional identities is particularly interesting from a data protection and privacy perspective. Processing an individual's full identity is a very intrusive action towards the data subject, and should be avoided as far as possible. Indeed, it is much more in line with the principles of proportionality and of data minimisation to use a person's partial or functional identity whenever possible.[1017]

**iv. Direct and Indirect Identification**

For the purposes of the European data protection and privacy framework, it is furthermore important to note that a person can be directly or indirectly identifiable (article 4 (1) GDPR). An individual is always directly identifiable when anyone can link personal data straight to a data subject, that is, where there are no

1012 The level of information deemed useful in this regard is evaluated differently in different countries.
1013 De Andrade et al. (2014), p. 5.
1014 Vandezande (2011), p. 2.
1015 Monteleone (2012), p. 5; Pocs (2011), p. 164.
1016 Article 29 Working Party Opinion 05/2014, p. 11 f.
1017 See also Chapter VII on anonymity below.

additional steps necessary to arrive at the individual's identity.[1018] For instance, whenever a person is identified by name, this is a direct identification.[1019] This classification is also not impacted if there are two people with the same name in a large sample.

Indirect identification means that a data subject can be identified after one or more additional steps are taken by which personal data is linked to him or her.[1020] This is for instance the case with information such as a phone number, IP address, or automobile license plate.[1021] These indirect identifiers often leave a very small group of people, such as a family or a workplace. For example, if a licence plate is the identifier, it is registered on one specific person's name, but this person's partner or grown children might also drive the car regularly. The same applies to a land line phone number, which identifies a residence rather than a person, but the group of people who will access this phone regularly is usually still very small.

However, identification of a person often depends very much on the context, and on the knowledge of the person who is concerned in the identification. As the CJEU termed it, "The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified."[1022] As the Article 29 Working Party points out,

> "A very common family name will not be sufficient to identify someone – i.e. to single someone out – from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom. Even ancillary information, such as 'the man wearing a black suit' may identify someone out of the passers-by standing at a traffic light."[1023]

The particular sample of persons concerned, and the context and circumstances of the identification are thus exceedingly important in the indirect identification

1018 Article 29 Working Party, opinion 4/2007, p. 13.
1019 Article 29 Working Party, opinion 4/2007, p. 13.
1020 Article 29 Working Party, opinion 4/2007, p. 13.
1021 See CJEU Case C-582/14 *Breyer* [2016], paragraph 41. See also Nicoll (2003), p. 99. See also the discussion of pseudonyms in Chapter VII below.
1022 Case CJEU C-582/14 *Breyer* [2016], paragraph 41. See also Karg (2015), p. 525.
1023 Article 29 Working Party, opinion 4/2007, p. 13; Article 29 Working Party Opinion 05/2014, p. 11 f.

of persons. For instance, a land line phone number has already been given as an example. If that phone number connects the residence of a family of five, one cannot be certain which family member was having a certain phone conversation. If, however, it is known that the phone call was made on a Wednesday morning, and it is known that one parent regularly works at home at that time while the rest of the household is at work or in school, the person making the call is identified.[1024]

The Article 29 Working Party has excellent explanations of both direct and indirect identification, which shall be quoted here in their entirety. First of all, direct identification is generally ascertained by linking information to the name of a person:

> "In order to ascertain this identity, the name of the person sometimes has to be combined with other pieces of information (date of birth, names of the parents, address or a photograph of the face) to prevent confusion between that person and possible namesakes. For example, the information that a sum of money is owed by Titus can be considered to relate to an identified individual, because it is linked with the name of the person. The name is a piece of information that reveals that the individual uses that combination of letters and sounds to distinguish himself and be distinguished by other persons with whom he establishes relations. The name may also be the starting point leading to information about where the person lives or can be found, may also give information about the persons in his family (through the family name) and a number of different legal and social relations associated with that name (education records, medical records, bank accounts). It may even be possible to know the appearance of the person if his picture is associated with that name. All these new pieces of information linked to the name may allow someone to zoom in on the flesh and bone individual, and therefore through the identifiers the original information is associated with a natural person who can be distinguished from other individuals."[1025]



1024 See in this context the comments made on linking of information below in Chapter VII.
1025 Article 29 Working Party, opinion 4/2007, p. 13; Article 29 Working Party Opinion 05/2014, p. 11.

Secondly, indirect identification relates to an individual, whose name might not be known, but about whom information of such a description was collected, that only one individual in a sample can be meant.

> "As regards 'indirectly' identified or identifiable persons, this category typically relates to the phenomena of 'unique combinations', whether small or large in size. In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be 'identifiable' because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others. This is where the directive comes in with 'one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity'. Some characteristics are so unique that someone can be identified with no effort ('present prime minister of Spain'), but a combination of details on categorical level (age category, regional origin, etc.) may also be pretty conclusive in some circumstances, particularly if one has access to additional information of some sort. This phenomenon has been studied extensively by statisticians, always keen to avoid a breach of confidentiality."[1026]

The concepts of direct and indirect identification are exceedingly important as a basis upon which to discuss specific data protection issues. It is particularly the indirect identification of data subjects which is a pivot of many problems which are part of the research problem addressed in this thesis. For instance, the linking of information and indirect identification play a big role in surveillance as discussed throughout this thesis, they are directly concerned in the sensitivity of financial data argued in Chapters V and IX, and they are finally the basis for the discussion of anonymity in the following Chapter VII.

1026 Article 29 Working Party, opinion 4/2007, p. 13. See also Boehme-Neßler (2016b), p. 420.

## d. The Protection of Identity

The foregoing sections have outlined the approaches to identity and identification in social sciences and, in contrast, in the law. The distinction between these two different disciplines is not, however, very stark. Indeed, the data protection legislation refers extensively to the concept of identity as it is applied in social sciences. In this way, the GDPR refers to identified or identifiable persons. By which factors an individual is identified is of no consequence for the application of the GDPR. Therefore, while objective factors such as names and addresses play an important role in this context, other factors of a person's identity can also come into play. In this way, the GDPR mentions "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of an individual (article 4 (1) GDPR).

It can therefore be stated that the legal approach towards identity is closely connected to the underpinnings brought in by social sciences. Indeed, the protection of an individual's identity, personality, and privacy is the very basis for the protection of personal data. In other words, the data protection legislation is designed in order to grant the individual the space for the development of his or her identity and personality.



This idea is for instance also illustrated by the concept of personality rights in German constitutional law. In brief, personality rights are a bundle of different rights protected by article 2 of the German constitution, which protects the right of the individual to freely develop his or her personality.[1027] One of those rights is the right to informational self-determination,[1028] which is the right under which personal data is constitutionally protected in Germany. The German system

1027 Article 2 GG reads as follows: „(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. (2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden."

This article may be translated as "(1) Everyone has the right to free development of his personality, insofar as he does not injure the rights of others and does not infringe the constitutional order or public morals. (2) Everyone has the right to life and bodily integrity. The freedom of the person is inviolable. These rights can only be limited based on a law." Translated by the author. The generic masculine form was retained from the original.

1028 This was first developed in the Census Decision of the German Constitutional Court, BVerfG, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 [1983].

therefore connects data protection and privacy directly to a person's personality and identity. While this link is not quite as obvious in European law, the foundations are the same.

It has already been established in the previous Chapter V that the right to privacy and human dignity are directly connected. Based on the foregoing, the identity of a person should be added to this connection in order to create a triad. Indeed, the three concepts of privacy, identity, and human dignity are intimately interconnected, each resting on and supporting the other two. It follows from the design of this framework that the identity of a person must be especially protected, along with the personal data and privacy as well as the dignity of an individual.

The law does not, however, follow this approach to its logical conclusion. It fails to protect the identity of individuals in several ways. In the first place, the data protection legislation fails to consistently protect spaces, or spheres,[1029] in which the individual may freely develop his or her personality. This development of one's personality best takes place where the individual is free from self-restraint,[1030] in privacy and protected from the observation and interferences by third parties. However, many individuals are almost constantly identified in everything they do, especially when a data subject uses internet services, to which he or she is indirectly identified through the IP address used, and which make extensive tracking very simple and inexpensive. As will be discussed in Chapter VII below, from a privacy perspective, anonymity is the best and simplest protection for an individual's identity. The data protection legislation allows for anonymity; indeed it demands it to some extent.[1031] The principles of data protection, particularly the principle of data minimisation, demand that an individual is only identified where this is necessary. But the law does not enforce anonymity, which results in a situation in which individuals are constantly identified and tracked, particularly in an online context. Indeed, the principle of data minimisation is largely reduced to a declaration without substantial effect.

Secondly, a person's identity is always closely related to sensitive information. Many of the illustrations given to explain the term identity above in both the social

1029 See the discussion of the Theory of Spheres in Chapter V (d) above.
1030 See by analogy the remarks made on the self-restraint of individuals caused by surveillance, Martini (2009), p. 841; Maras (2012), p. 74.
1031 See the following Chapter VII.

sciences as well as the legal context were referring to aspects of an individual's identity which at the same time fall into the categories of sensitive data. As has been explained in Chapter V above, the data protection legislation principally bans the processing of sensitive data (article 9 (1) GDPR). However, this ban is accompanied by a list of ten exceptions, some of which are rather broad (article 9 (2) GDPR). Member States may furthermore introduce further exceptions concerning the processing of biometric, genetic, and health data (article 9 (4) GDPR). The ban on the processing of sensitive data is therefore effectively reduced to being a ban in name only. The close connection between categories of sensitive data and a person's identity does, however, demand especial protection of such information.

These two reasons alone allow for the conclusion that the data protection law falls short of a proper standard of protection for a person's identity. The foundation of data protection on privacy, identity, and human dignity would demand a high level of protection, and indeed the outline of tools to protect a person's identity appears in the principles of data protection and in the protection of sensitive data. However, the standard of protection is watered down by the failure of the GDPR to consistently protect spheres within which the individual is not identified.



One of the conclusions which can therefore already be drawn at this point is that the law does not protect a person's identity as consistently as it ought. This shortcoming causes a decreased standard of protection of the human rights to privacy and data protection. Were the data protection legislation designed in such a way as to protect an individual's identity properly, this protection would result in a higher level of the protection of privacy and personal data. This higher protection would in particular substantially increase the protection of sensitive data, and fill the principles of data protection with additional meaning.

## e. Privacy and Identity in Financial Transactions

It has already been mentioned at the beginning of this chapter that a person's social and personal identity as well as the legal concept of a person's identity all play a role in financial transactions. This section is dedicated to the details of this connection.

**i. The Conventional Banking Sector**

The Anti-money laundering Directive provides that obliged entities must fully identify all of their customers. Compared to virtual currencies and informal transaction systems, banks are relatively easily supervised and compliance with this legal obligation can be ensured. In general, banks therefore also have a rather good record in compliance with these particular obligations, although the cooperation between financial institutions and Financial Intelligence Units is not free from friction.[1032]

Any customer of a bank or another financial services provider is fully identified with the help of a government issued ID document. Therefore, all movements of funds can in principle easily be traced to and from this person's account.[1033] But what is particularly interesting from an identity perspective is the amount of information a bank, or anyone in possession of a transaction record of only a few weeks can potentially infer about a person. A person's bank account allows the generation of a very detailed about a person, and that person's private life and daily habits. A bank account will register the person's income, and from the data on the sender of that income, the employer can be determined. Furthermore, the bank already has a person's address registered in the customer database, but either rent or mortgage may be deducted from that person's account, too, allowing to draw conclusions on the person's housing situation and financial well-being. The bank account will furthermore register other periodical payments, such as alimony to an ex-partner, or pocket money to children. The amounts and origins of any debts can also usually be inferred from the financial movements of a person.

Furthermore, and more problematically, it has already been mentioned that there might be expenses and financial movements which allow deductions about information about a person which reach into the realm of sensitive data.[1034] Sensitive data is a special category of personal data, already introduced above. The different types of sensitive data are defined in article 9 (1) of the GDPR. This provision of the GDPR specifically interdicts the processing of particularly sensitive categories of data, such as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,

1032 Wensink et al. (2017), p. 151.
1033 See the discussion of customer due diligence obligations in Chapter II above. See also Rossum et al. (1995), p. 41 ff.
1034 Article 29 Working Party, Opinion 14/2011, p. 26.

[…] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

It has already been pointed out several times in this chapter that the processing of these categories of data are in principle forbidden by article 9 (1) GDPR, but this prohibition of processing does not seem to affect the fact that financial transactions may inadvertently include data about a person which concern sensitive information.[1035] If a person donates money to a political party, or to a foundation closely associated with a certain political belief, much can be inferred about the donor's political affiliations. The same is true for religious and philosophical beliefs. Religious institutions often depend to a large extent on donations, and if those are made electronically, they will leave a trail between an institution linked to a certain religious community and the owner of a certain bank account. If a certain trade union periodically deducts a certain amount of money from a person's account, the assumption that this person is a member of that union is not very far-fetched. If a person regularly spends a lot of money at pharmacies and medical services providers, information on these payments may lead to accurate assumptions on a person's health. Finally, payments made to sex shops and gay bars may concern a person's sexual orientation, and allow rather intimate insights into a person's sex life.



Of course, a payment made to a gay bar does not automatically and certainly mean that the customer is also homosexual. Most casual gay bars are open to the public and also welcome heterosexual customers. Not everyone who donates to religious organizations is a member of the same faith as that organization. An atheist may well donate to a fundraiser for an orphanage operated by a catholic order. The fact is, however, that it will be speedily assumed that a visitor or a gay bar is homosexual, and that a financial donation to a religious organization reflects the faith of the donor. In many cases, such an assumption is accurate. Another example given above makes this point even clearer, as there is not really another explanation for regular deductions by a big trade union from a person's bank account other than that this person is a member of said union.

1035 Article 29 Working Party Opinion 14/2011, p. 26; Wasserstrom (1984), p. 326.

The categories of sensitive data and the ban on the processing of such data exist for a reason.[1036] The ban on the processing of those categories of data serves to protect people from stigmatization, exclusion, and discrimination. There are many persons who will face discrimination if details of their religious belief or their sexual orientation were to be made known to third parties. Even today, unfortunately not everyone is tolerant of homosexuals or transsexuals, and people accused of homosexuality can still face lynching, long prison terms, or the death penalty in some countries. Even in the European Union, the suspicion of homosexuality is still costing many people their jobs, social position, or political office. In the same way, freedom of religion is not realized in large parts of the world. Conflicts between religious groups annually lead to countless deaths worldwide. In some countries, conversion away from Islam is punishable by death, and while this is not the case on the European continent, members of the immigrant communities from these countries, even after several generations, must tread carefully. Everywhere in the world, including in the EU, religious intolerance is a sad reality, and discrimination is often a fact of life for members of religious minorities. These examples illustrate some of the reasons why the lawmaker has decided for the ban of the processing of such data.

All this information is clearly personal data revealing sensitive information, and, it must be repeated, in principle, the processing of such information is banned. In principle, banks process personal data lawfully on the basis of article 6 (1) (b) GDPR, "processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract". However, this exception applies only to ordinary personal data. It does not cover sensitive information, which is generally processed inadvertently by service providers.

Clearly, there is a divide between the law and reality in this case.[1037] The data protection laws define a complete ban of processing of certain categories of data (with limited exceptions), in order to protect the data subject as far as possible from the potential harm outlined above. Equally clearly, this data must be processed in order for the service provider to provide its financial services to the customer, i.e. to process a transaction. At the same time, however, the aforementioned

1036 See also Benn (1984), p. 226 f.
1037 See in this context also the fifth concern discussed in Chapter IX below.

obligations of the bank to monitor transactions, and to transmit information to the Financial Intelligence Unit are not impeded by the fact that sensitive categories of data are affected in this monitoring and reporting practice.[1038] This exposes a bank customer to the danger that transaction records also containing sensitive personal information is transmitted to the authorities. The law does not provide for additional safeguards to protect the customer's sensitive information in such situations. This is clearly a grave oversight in the drafting of the Anti-money laundering Directive, and also of the GDPR.[1039]

Finally, it should be stated that banks are required to keep all the information collected safe, according to their obligations under the GDPR and due to their contractual obligations to the customers. It is furthermore stipulated in Article 41 (2) 4AMLD that the data collected under the terms of the Directive must not be used for other purposes, specifically including commercial purposes. However, were a third party to gain access to the collected transaction history of a customer[1040] of merely a few weeks or months, all the problems outlined above would instantly manifest themselves. A stronger protection against such a relay should therefore be provided for by law. The ban on the processing of sensitive data may play a meaningful role in such a protection, if it were to be interpreted in a way to protect the customer from the sharing of information about him or her that may potentially reveal information relating to one or more categories of sensitive data.



In addition, inadvertent data leaks of a very high magnitude are a grave threat.[1041] Data is leaked daily from large companies, and a bank is surely a very attractive target for attackers. Vulnerable data would not only be a customer database with names and addresses as well as credit card information and bank account numbers, but also the information to be gleaned from financial movements, as just

1038 Article 29 Working Party, Opinion 14/2011, p. 26.

1039 See in this context also the CJEU's critique of a similar oversight in the Passenger Name Records agreement, Opinion 1/15 *PNR* [2017], paragraphs 165-167, to be discussed in more detail in Chapter VIII below.

1040 See in this context specifically the terms of the PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127. The PSD2 regulates access to financial data by third financial services providers.

1041 See, in this context, also Schwartz (1968), p. 751.

described above. Such information would be useful for advertising purposes and fraud, but one should not forget that persons in specific circumstances might also be vulnerable to blackmailing.

In this context, it must be stressed that when a high level of data protection, privacy, and identity protection is desired, cash offers a level of anonymity unrivalled by any of the three systems discussed here.[1042] While all financial movements made by a customer electronically are stored by the banks, and customer due diligence measures are applied to them, it must again be emphasised that any transaction made in cash is anonymous. The information recorded by a bank on the withdrawal of cash, which is the main connection between the banking sector and cash transactions in this context, is limited to a time stamp and the ID of the machine from which the withdrawal was made. What happens with the cash afterwards is not recorded anywhere. The customer might use it to buy groceries, in which case the banknotes might be paid into the store's bank account at the end of the business day. But it is also likely that the cash is paid out as change to another customer and begins a long cycle before it is again paid into a bank. Of course, instead of buying groceries, the cash might also be used for buying drugs at a street corner, or to pay a corrupt police officer. Such a transaction would be completely anonymous and there would be no possibility to trace the banknotes back to the parties to that transaction by simply examining the notes. These thoughts on anonymity and challenges encountered by the law enforcement authorities will be further expanded in the following Chapter VII.

**ii. Virtual Currencies**

A person's social and personal identity can come into play when the choice for a particular financial transactions system is made based on the user's personal identity. The reasons why users may prefer virtual currencies to other transaction systems have been spelled out in a previous section.[1043] Several of them connect to the personal and social identity of the user. While for example the speed and cost-effectiveness of transactions are certainly main factors, there are also several issues pertaining to the users' identity in this context. Bitcoin, for instance, particularly appeals to many users who have an interest in cryptography and computer science in general, and many prefer the Bitcoin system because of its open structure and

1042 Dwyer (2014), p. 9. See also Chapter III above.
1043 See section (d) of Chapter III above.

the lack of a central authority. Also, of course, there is a group of users who wish to buy or sell illegal material, and wish to use virtual currencies for this purpose.

The social identity of users of virtual currencies is largely based on the last two elements. The image of virtual currencies in the mind of the general public is dominated by the extensive media coverage of police action against the sale of drugs through the dark web, and particularly the initiative against the online market place *Silk Road*[1044] and several of its successors. Therefore, virtual currencies and their users are also often regarded with suspicion.

Virtual currencies also bring an interesting perspective about the legal identity and identification of the users. As has already been criticised in the previous chapters, the technical architecture of the system is often misunderstood and the system is erroneously described as 'anonymous'. This, however, is not strictly accurate. In fact, anonymity was never a desired feature of the architecture of the blockchain system.[1045] The common impression that virtual currencies function anonymously is for the most part an illusion created by the fact that observers and even many users of these systems do not thoroughly understand the concept of anonymity, nor the technical infrastructure of the virtual currency they are using.[1046]



Bitcoin is a prime example for this misunderstanding. As has been described above. the blockchain records information about all transactions and makes it available to the public. The ledger contains information on the wallet files used in each transaction, but not the name and address of the person owning that wallet file. This lack of a clear name in the records is the root of the illusion of anonymity. However, the identifier of the wallet file acts much like a pseudonym in this case. Each wallet can be linked to a person, the user who controls the wallet and owns the bitcoins stored therein. If the wallet address is changed for every transaction, the wallet address is a person's transaction pseudonym.[1047] This option allows for maximum security. But if the wallet address is not changed, and many transactions are carried out with the same wallet, the pseudonym degenerates to a role pseudonym. The sort and amount of transaction carried out with the

1044 Raman (2013), p. 67 f.; Dowd (2014), p. 70 ff.
1045 *Nakamoto* cited in Dwyer (2014), p. 9
1046 Cf. Dwyer (2014), p. 9.
1047 See the following chapter for a detailed discussion of the different types of pseudonyms. See also Rückert (2016), p. 8.

same wallet determines the vulnerability of the pseudonym, i.e. how unique those transactions are and if and how they can be linked to an offline identity. These notions will be expanded upon in the following Chapter VII.

Instead of granting anonymity, the openness of the system and the availability of information about all transactions via the blockchain in fact makes users of virtual currency systems very vulnerable to identification and to having their entire transaction history exposed to the general public.[1048] This danger was recognized from the very start by the architects of the Bitcoin system: *Satoshi Nakamoto* warned that there could be "some linking with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner."[1049] It would be theoretically possible to create a database with all known public keys, and linking them to one another as well as to information from other sources.[1050] Such a database, if supplied with a sufficient amount of third party information, would be a "potentially serious threat" to a person's privacy.[1051]

Information linking a wallet to a real world identity is can, however, be found rather easily. There are, for instance, several large non-profit organizations accepting donations in virtual currencies. Their wallet addresses are publicly available on their websites. Other identified users are the ubiquitous gambling services and some large commercial entities, such as online stores and exchange services. Both of the latter entities may keep information on the identity of their users, which may include names, payment details, IP addresses, email addresses, and shipping addresses.[1052] Should an attacker gain access to any of those data bases and link this information to other publicly available information, a large segment of the virtual currency environment would be at risk of having their identities exposed.[1053]

1048 Reid/Harrigan (2012), p. 11. See also Rückert (2016), p. 12 f.
1049 *Nakamoto* cited in Reid/Harrigan (2012), p. 11. See also Article 29 Working Party Opinion 05/2014, p. 11 f.
1050 Reid/Harrigan (2012), p. 15; COM (2016) 450 final, p. 9.
1051 Reid/Harrigan (2012), p. 15. Note that such a database is precisely what the Commission envisioned in its proposal for a fifth Anti-money laundering Directive, see COM (2016) 450 final, p. 9.
1052 Reid/Harrigan (2012), p. 15; Raman (2013), p. 68.
1053 Reid/Harrigan (2012), p. 15.

For a maximum amount of security, users generally have recourse to third party anonymization features.[1054] There are wallet services offering storage of virtual currency units with maximum identity protection, and there are mixing services that obscure the trail of bitcoins from one address to another by shuffling the funds from several transactions up with each other.[1055] Those services can be used to maximise the protection of the user's privacy and identity.

The privacy afforded by the Bitcoin system is largely based on the decentralization of the system. There is not a single entity which creates, administers and has access to a central database containing all information on customers and their transactions.[1056] This is the fundamental difference between a virtual currency system and a bank. This decentral structure is furthermore a bar to the central application of customer due diligence measures.[1057] While all transactions carried out within a bank's infrastructure are scrutinized according to the standards demanded by the Directive, virtual currency environments remain unencumbered by such scrutiny. Nothing in a virtual currency system will stop a user from transferring funds, for instance contrary to an embargo.[1058] Virtual currency units or wallets in a virtual currency environment cannot easily be frozen if an embargo is violated or if a customer is on a blacklist.[1059] Similarly, transactions are not blocked by a central agency.[1060] In the famous *WikiLeaks block*, for example, credit cards discontinued to process donations to the platform. Such a payment blockade cannot be exacted from a virtual currency system.[1061]



It is difficult to compare the level of financial privacy that can be achieved using Bitcoin with the level that can be provided by banks. In Bitcoin, one's transactions are generally carried out in plain view of the public, and the only protection of the user's identity is the pseudonymity of the wallet file. Using a virtual currency system with absolute security for one's privacy and identity is considered impossible.[1062]

1054 Filippi (2014), p. 2.
1055 Filippi (2014), p. 2; Möser/Böhme/Breuker (2013), p. 5.
1056 Dwyer (2014), p. 9; Raman (2013), p. 68. See in this context also Maras (2012), p. 72; Sorge (2007), p. 104.
1057 Rückert (2016), p. 12 f.
1058 Böhme et al. (2014), p. 5.
1059 Transferring the concept of blacklists to virtual currencies has been discussed, but was rejected by the majority of the Community. See Möser/Böhme/Breuker (2013), p. 11 f.
1060 Böhme et al. (2014), p. 5; Korff (2014), p. 39 f.
1061 Dowd (2014), p. 75; Sorge/Krohn-Grimberghe (2012), p. 482.
1062 Dwyer (2014), p. 9; Murck (2013), p. 96.

However, users can achieve a high level of privacy if they use the system carefully and add anonymization features.[1063] In a bank, the situation is greatly different. The customer's name and address as well as his transaction history is known to the bank, as one central entity. However, at the same time banks always work with fiat currency, including cash. Thus, banks keep complete records about their customers' identities, and compile a long and extensive history of each customer's financial transactions. But they can necessarily only keep records on transactions routed through their systems. As has already been explained above, cash transactions therefore remain anonymous.

Transactions in virtual currency systems can therefore be compared to cash transactions.[1064] If one uses cash, the ATM records when, where and how much cash was paid out to the customer. But what the customer does with the money that was withdrawn is not monitored by the bank through the application of customer due diligence measures. Virtual currencies work very similarly in this respect:[1065] An exchange service pays a user a certain amount of virtual currency in exchange for fiat currency. But what the user does with the virtual currency is not monitored by that exchange service.

**iii. Informal Value Transfer Services**

In a Western European context, the standardized banking system is so dominant that it is very difficult for any member of the mainstream society not to use it. A bank account is needed to receive wages and/or social benefits. A bank account is needed to pay taxes, rent, and insurances.[1066] Attempting to use a different payment system for any of these services will raise eyebrows at the least, and will likely be declined and met with suspicion. The deviation from this standard can, however, be a strong link to an individual's social and personal identity.

In the case of Hawala, the user's choice to use that transaction system can often be linked to the user's personal identity.[1067] In the previous chapters, it has already been shown that the choice for a Hawala transaction is particularly influenced by the cultural preference of the user. Main factors are the reliability, speed and low costs of

1063 Murck (2013), p. 96.
1064 Kaiser (2016b), p. 4 ff. See also Luther (2016), p. 402.
1065 Kaiser (2016b), p. 4 ff.
1066 Datta (2009), p. 335.
1067 See in this context also Razavy/Haggerty (2009), p. 145.

transactions, and also the fact that Hawala serves rural and remote areas often better than the general banking system. However, the importance of the fact that a user and a hawaladar are generally members of the same ethnic community should not be underestimated. The same is true for the fact that Hawala transactions are Sharia compliant, often connecting to the user's religious beliefs. There are many users of the Hawala system who will choose that system because of those latter factors, i.e. because they share the same culture and heritage with the hawaladar and thus find it easier to communicate with and trust this person. Furthermore, if a user follows the teachings of Islam very strictly, not many financial services other than Hawala will satisfy the user's demands regarding the character of the operations.[1068]

These are clearly cultural factors which are a part of the user's personal identity. They are, however, also a part of the user's social identity, insofar as they can be perceived by the rest of society. The society at large may perceive the user's belonging to a certain ethnic group and cultural heritage, as well as his or her being a Muslim. Based on the recent global wave of terrorism, a person's belonging to a Middle Eastern ethnic community and being Muslim can quickly lead to that person being regarded with suspicion by other segments of society. Hawala is an especially severe case in this context, because of the negative associations created between Hawala and terrorism.[1069] As has been shown earlier, the largest part of the European population has probably never heard of Hawala, but there is a segment of the population which associates Hawala only with terrorism and believes Hawala to be a tool used purely to finance terrorist activities. Therefore, there is a considerable danger that a user's association with the Hawala transaction system can quickly create the social identity and negative labels of extremist, terrorist, or terrorist financier.



The anonymity inherent in cash transactions also plays a role in Hawala transactions. Cash features heavily in Hawala transactions, not least because many countries in which Hawala is most dominant are not endowed with well-developed banking infrastructures, which rules out electronic banking. Thus, Hawala stands apart from banks in that transactions carried out with the help of cash through the Hawala network hardly intersect with the banking system. The records kept by banks will thus reveal no information about the involvement of a customer

1068 For more details on the compliance of Hawala with the Sharia, refer to Chapter III above.
1069 Redin/Calderón/Ferrero (2012), p. 8; Article 29 Working Party, Opinion 14/2011, p. 19.

in the Hawala network, either as client of a hawaladar, or even when the client operates as a hawaladar himself. Virtual currency systems are even more starkly contrasted with Hawala, due to the open records of the blockchain technology and the emphasis on technology.

But how well do hawaladars identify customers and keep records of transactions carried out by them? Many writers claim that Hawala is necessarily an anonymous transaction system.[1070] This statement needs to be nuanced, however. The records of hawaladars are indeed generally much less detailed and limited to information necessary to a transaction, simply because it is expedient to limit record keeping to what is necessary. In theory, a hawaladar does not need to record the identity of the sender to carry out the transaction. It would suffice to record the identity of the hawaladar with whom this transaction was carried out, in order to balance the books between those two hawaladars later on. And while it is often repeated that the Hawala network is based on trust between the hawaladars, it can be assumed that each hawaladar works hard to maintain that trust extended by his colleagues. Each hawaladar must thus keep very minute records on how much money he owes to his colleagues, and how much money he is owed by his colleagues, and bring each of these records up to date after every transaction.[1071] Furthermore, a diligent hawaladar would keep the information received about the recipient in each transaction, in case of a misunderstanding about the identity of the recipient. The information about recipients would also be helpful if a dispute arises between two hawaladars and they need to compare books in order to find the mistake. The above is primarily suggested by common sense. These are the records that it would be logical to keep in the interest of a smoothly running business. Records from police investigations into Hawala suggest that hawaladars think along much the same lines.[1072]

Some authors have insisted that the use of the Hawala system affords anonymity to its users, but this is most likely also a result of an imperfect understanding of the term anonymity. The difficulties many people have with the concept of anonymity have already been outlined above in connection with virtual currencies, and will be gone further into in the following chapter. It would be more correct to say that Hawala affords much privacy to users. A high level of privacy is afforded by Hawala

1070 For instance prominently Raphaeli (2003), p. 70. See also Redin/Calderón/Ferrero (2012), p. 11 with further references.
1071 Redin/Calderón/Ferrero (2012), p. 11; Passas (2006), p. 50 f.
1072 Soudijn (2015), p. 263.

because a hawaladar's books cannot generally be accessed by any third party, and the manner of bookkeeping differs greatly from one hawaladar to another.[1073] The records are not designed in a way to be understandable by any third party also because no third party is intended to be granted access: a hawaladar's books are generally not reviewed by auditors and external consultants.[1074] Furthermore, there are communities served by Hawala in which identification documents are either not generally available, or which the customer prefers not to show because, for instance, he or she might be an undocumented migrant.[1075] In the words of Lascaux,

> "Lack of bureaucratic formalities and ease of identity verification procedures (value transfer can be arranged under assumed name) attract individuals who prefer anonymity, do not place trust in the official banking services or experience difficulties with filling out their requisite forms."[1076]

All these factors lead to customer due diligence measures being dismissed as "a pointless imposition by a foreign power"[1077] by users and proponents of Hawala. On the other hand, these same factors lead to increased suspicion by the opponents of the system. The fact that the records are not kept in a standard form but rather in an abbreviated form of the country or region of origin of the hawaladar and his main customer base is often referred to as the "intrinsic opaqueness" of Hawala.[1078]

Finally, it should be stressed that of course, not all hawaladars operate underground. Numbers provided by the FATF show that in countries where Hawala is legal, customer due diligence obligations can be imposed upon hawaladars in the same way as on their legal counterparts (such as *WesternUnion* and *MoneyGram*).[1079] Of course, not all hawaladars accept this regulatory burden, or carry out their obligations in a manner which would satisfy law enforcement agencies. Lascaux notes that in the United Kingdom,

1073 Redin/Calderón/Ferrero (2012), p. 11.
1074 Redin/Calderón/Ferrero (2012), p. 11.
1075 Redin/Calderón/Ferrero (2012), p. 11.
1076 Lascaux (2015), p. 93.
1077 *Razavy and Haggerty* cited in Redin/Calderón/Ferrero (2012), p. 11. See also Pieke/Van Hear/Lindley (2007), p. 349 f.
1078 Lascaux (2015), p. 93.
1079 FATF Hawala (2013), p. 49 f. See in this context also Reimer/Wilhelm (2008), p. 235.

> "financial authorities note that Hawala operators tend to underreport suspicious transactions and break at least some of the regulatory principles concerning implementation of anti-money laundering policies, verification of the clients' identities, and retention of legible transaction records."[1080]

However, similar critique is made of the obliged entities which compose the conventional banking sector,[1081] so the Hawala system is certainly not unique in this regard.

## f. Conclusion

The foregoing has made it clear that the concept of identity can be understood in widely different ways, depending on which interpretation is given to the word. Both of the interpretations of identity in law and social sciences outlined in this chapter depend on the similarities and differences between an individual and other individuals in a group, though widely different parameters are used for this distinction.

To repeat the essence of the analysis made, it can be said that a personal identity describes a person's view of him- or herself, and how this individual expresses the differences between him- or herself and the rest of society. Factors that come into play here are specific characteristics, beliefs, visions or principles, or attributes, that a person considers to be especially expressive of him- or herself.[1082] Anyone can thus identify these characteristics in him- or herself and in others, and thus invent or discover a personal identity which is unique to this individual and subjectively distinguishes him- or herself from the personal identities of all other members of society.

The differences between an individual's personal and social identities shows that a person's subjective view of his or her unique personal identity is not necessarily perceived in the same way by other members of society. The social identity of a person is essentially society's response to an individual's personal identity. A

1080 Lascaux (2015), p. 93.
1081 See the remarks made in this context in Chapter IV (b) above.
1082 Fearon (1999), p. 2.

person's social identity is that person's perceived membership of a group of persons, based on a certain characteristic or attribute that this person shares with the other members of the group.[1083] Other members of society largely determine according to which common characteristic or attribute a group is formed, and the individual may have little control over his or her membership in a certain group. Then, often, prejudices are attached to a person's membership in that group. The most common groups are formed along the lines of gender, skin colour, and heritage, and other attributes easily visible in an individual's personal appearance.

Finally, a person's identity in the sense attributed to it in the data protection legislation is primarily the way an individual is distinguished from all other individuals of society. While this is most often achieved by using objective factors, either individually or in combination, such as a citizen identification number, the name of a person, and his or her date and place of birth, the objectivity of the identification is broken up in some areas where any identifier may be used. The law very clearly references a person's social and cultural identity, which bridges the gap between the social and legal concepts of law. Data protection law in this context must function as a protection of the individual from the negative consequences of prejudice and stigma, but there are severe weaknesses to this protection, such as the fact that a person's name, which is not a piece of sensitive data, can make a very clear reference to a person's ethnic heritage, which is a piece of sensitive data. Aspects of these discrepancies are going to be the subject of further reflections in the following chapters.



The notions of an individual's personal and social identities as well as the notion of an identified or identifiable person will strongly influence the analysis of the interferences of the Anti-money laundering Directive with the rights to privacy and data protection in Chapter IX. The notion of identity is an important factor in the discussion of the right to privacy, and is therefore constantly present in the analysis. The identification of all customers of the financial industry will be the subject of the third concern to be discussed in Chapter IX. The fifth and sixth concerns also have a strong link to the notion of identity.

Finally, in section (d) of this Chapter VI, it has been argued that the notion of identity is intimately connected to the right to privacy and to human dignity. It was

1083 Fearon (1999), p. 2.

criticised that the data protection legislation does not consistently protect spaces in which the individual can freely develop his or her identity. Such spaces would have to be protected by anonymity. The concepts of anonymity and pseudonymity are the subjects of the following Chapter VII.

# Chapter VII

## Anonymity and Pseudonymity

## Outline:

a. Introduction
b. Anonymity and Pseudonymity
    i. Background
    ii. Anonymity and Privacy
    iii. Different Types of Pseudonymity
c. Anonymity in theLaw
    i. Anonymity as a Right
    ii. Pseudonymisation
    iii. Anonymity as Non-Identifiability
    iv. Potential Identifiability
    v. A Limit to Anonymity
    vi. Anonymity in the Anti-money Laundering Directive
d. The Unidentified Data Subject
    i. The Interest in Anonymity
    ii. A Holistic Approach to Identification
    iii. A Right not to be Identified?
e. Anonymity and Pseudonymity in Financial Transactions
    i. The Conventional Banking Sector
    ii. Virtual Currencies
    iii. Informal Value Transfer Services
f. Conclusion

## a. Introduction

In the previous chapter, it has been shown how a person's identity affects an individual's daily life in society and how an individual's identity can influence his or her choice for a certain system of financial transactions, as well as some of the consequences of this choice. One way to protect oneself from the possible negative consequences of prejudices and stigmatization often inherent in social discourse, and to protect one's personal identity in a social context, is to use pseudonyms or to try to remain anonymous whenever possible.

'Anonymity' and 'pseudonymity' are terms that are often used without a clear understanding of the underlying concepts. In the understanding of many members of the public, anonymity simply means that a person's name is omitted from information about that person, or information submitted by that person. Similarly, pseudonymity seems to be often understood simply as a person's going by another name than the name printed on that person's identity card or passport. Both concepts, however, are much more complex than these two simple examples would suggest.



*Anonymous* is a word derived from the Greek word *ἀνώνυμος*, meaning "Nameless, having no name; of unknown name",[1084] and the entry for the word *anonym* describes "A person whose name is not given, who remains nameless".[1085] In the words of *Paul De Hert*, "There is anonymity when the individual finds freedom from identification."[1086] The word pseudonym is derived from the Greek *ψευδώνυμος*, meaning a "false or fictitious name".[1087] In contrast to an anonymous person, a person is *pseudonymous* if he or she is "Bearing or assuming (esp. writing under) a false or fictitious name; belonging to or characterizing a person who does this",[1088] and thus a *pseudonym* is simply "A false or fictitious name, esp. one assumed by an author; an alias."[1089]

1084 Oxford English Dictionary, Third Edition 2010, s.v. "anonymous".
1085 Oxford English Dictionary, Third Edition 2010, s.v. "anonym".
1086 De Hert (2003), p. 47.
1087 Oxford English Dictionary, Third Edition 2010, s.v. "pseudonym". See also Froomkin (2003), p. 9.
1088 Oxford English Dictionary, Third Edition 2010, s.v. "pseudonymous".
1089 Oxford English Dictionary, Third Edition 2010, s.v. "pseudonym".

This corresponds with the popular and sometimes misleading notion of the word as explained above. However, the definition loses its apparent clarity immediately when one asks whether or not anonymity depends on the name alone. Is a person really anonymous if he or she can be identified by other information pertaining to him or her, other than the name, such as his or her face or other characteristic traits? In the following section, the background and the implications of the concept of anonymity will be explored.

The connection to anti-money laundering legislation becomes obvious when the remarks made on the duties to identify each customer are recalled to mind. The Anti-money laundering Directive specifically demands that all customers of obliged entities must be identified, and that anonymous accounts and passbooks are prohibited.[1090] This comprehensive identification of all users of financial services is, however, in direct opposition to the values of data protection and privacy. To optimally protect one's privacy and personal data, one will wish to remain anonymous and unidentified as much as possible. Discussing this conflict is the purpose and centre of this chapter.

This chapter is organised as follows. In the first place, the concepts of anonymity and pseudonymity are to be explained in detail (b). This is followed by a discussion of these concepts as they recur in the European data protection framework (c). Finally, the role played by anonymity and pseudonymity in financial transactions is to be examined. This concerns particularly the options open to users of each transaction system of concealing their identities. In this way, the present chapter builds upon many concepts introduced in the previous chapter, and should be read in conjunction with it.

## b. Anonymity and Pseudonymity

### i. Background

In general terms, anonymity can be described as the situation in which a person is only described in such a way as to not be distinguished from other persons in a given group.[1091] The group's mark-up is important for an individual to achieve

1090 See the discussion on identification in Chapter II above.
1091 Köpsell/Pfitzmann (2003), p. 17; De Hert (2003), p. 47.

anonymity. It is more difficult for an individual to remain anonymous if the group is small and heterogeneous than if it is large and rather homogeneous.[1092] This means that there must always be a group for anonymity to be a possibility: If a group of people consists of only one individual, that individual is naturally the one concerned; there is no chance of his or her identity being mistaken for someone else's.

Anonymity is usually not absolute. In theory, a person's anonymity can be absolute, in the sense that there are conceivable scenarios in which a person's identity can never be established beyond reasonable doubt. However, in most circumstances, it is hardly possible to exclude the possibility of being identified, even in a large, rather homogeneous group of people. The reason for that is the large amount of known and unknown variables that real life injects into all human interaction, and the uncertainty of how those variables can be explored and combined in the future.

Pseudonymity, on the other hand, is not a method used in order to entirely rule out identification.[1093] Indeed, many different types of pseudonymity exist, which form a scale of shades of grey between identification and anonymity.[1094] In principle, pseudonymity means that one's real-world full identity is hidden, so that a person's pseudonym can be used to distinguish a person from others without needing to resort to that person's identity. The concept of pseudonym is often used to keep different aspects of a person's life separated.



When an attacker tries to de-anonymise a person, or tries to link a real-world identity to a pseudonym, the first step is generally to aggregate all information that is known of the target. The strength of a person's safeguards for anonymity or pseudonymity always depends on a potential attacker's knowledge of the target, of the group as a whole, and of circumstances which may connect a person to a particular event. In order to find the real identity of a person, an attacker will collect as much information about that person and then try to link this information to only one person in the group.[1095] When the attacker learns one piece of information about a pseudonymous or anonymous person, he will search for persons to whom

1092 Köpsell/Pfitzmann (2003), p. 17. See also Walden (2003), p. 153 f.
1093 Article 29 Working Party Opinion 05/2014, p. 10.
1094 See the typology discussed below.
1095 Köpsell/Pfitzmann (2003), p. 17.

this information can be linked. The more information the attacker collects, the smaller the group of persons to whom all pieces of information can be linked. Eventually, there is only one individual left to whom each piece of information applies. When that happens, the previously pseudonymous or anonymous person is identified. The amount of information needed to identify a person depends, as was stated above, on the amount of members in a given group and the degree of homo- or heterogeneity of the members of the members. In a small, heterogeneous group, fewer pieces of information will be needed to identify any one member than in a large and homogeneous group.

**ii. Anonymity and Privacy**

The interest in using pseudonyms or remaining anonymous is ancient. However, the interest in protecting one's identity seems to have moved into the foreground particularly over the last few years.[1096] The ubiquity of the internet and the possibility for large data collections has had a deep impact on people's privacy,[1097] and many people, upon being made aware of the processes taking place, take active measures in order to hide their identity from attackers on the internet.

Anonymity and the perception of this concept among the people is in a process of change. In the not too distant past anonymity was essentially the general condition in society.[1098] The average person was known only to a limited amount of people intimately, with a slightly larger amount of people to whom he was known by name and/or by sight. If one goes back far enough, before the ubiquity of photographs, when passports only contained vague descriptions of the outward appearance of the bearer, if any, one's identity could potentially be hidden with the simplest measures.

It was also much harder to track people's behaviour before the days of the internet compared to today.[1099] Mass-media information was consumed via broadcasts from radio and television stations, or via newspapers. The providers of none of

1096 See also Petri (2010a), p. 26 f.
1097 Prantl (2016), p. 349.
1098 See also Brandeis/Warren (1890), p. 196; Froomkin (2003), p. 21 f.
1099 Naturally, surveillance and other intrusions outlined in this section have a long history and predate the modern technological advancements by centuries or in some cases even millennia. However, it cannot be denied that the ubiquity of identification mechanisms and surveillance in place today is only rendered possible by the immense data processing infrastructure which has been developed wihtin the past several decades.

those media were in a position to track who has received which information, as access to each of those media was readily available, and the information could not be tailor made for each consumer: each issue of a given newspaper was the same, rather than tailored to the presumed preferences of each reader. Similarly, the postal service could not scan the contents of one's private communications for advertising purposes. Searching paper records was a tedious, time-consuming activity. And finally, payments were made almost exclusively in anonymous cash.[1100]

As all these examples show, collecting information about someone, and linking information to a specific person, was much more difficult only a few years ago. Anonymity was more of the standard, and identification the exception. Only the small set of persons to whom a person was previously known or made known would be able to identify the person without his or her knowledge. To identify oneself, a person would typically show an official document, such as an identity card or passport, and the official to whom that person identified himself would compare the picture on the card to the face he saw.[1101] Human error and the rather low capacity of human memory naturally always allowed a degree of anonymity to persist.[1102]



The internet has had a remarkable impact on this condition.[1103] The sudden increase in the availability and accessibility of this technology opened unprecedented possibilities for data processing.[1104] The enormous amounts of available data need no longer be searched by hand, but may be searched and filtered by keywords, and can be evaluated automatically.[1105] Furthermore, the process of identification of a person can now more readily be carried out covertly, unknown to the target while it is happening.[1106] While before, one had to actively account for one's identity by producing ID documents, today, modern technologies such as face recognition

1100 Köpsell/Pfitzmann (2003), p. 13 f.
1101 See in this context Monteleone (2012), p. 4 f.
1102 Köpsell/Pfitzmann (2003), p. 13 f. See also Grijpink/Prins (2003), p. 251; Baum (2011), p. 595.
1103 Reddick/Chatfield/Jaramillo (2015), p. 132. See also Karg (2013), p. 76; Richter (2016b), p. 582 f.
1104 Article 29 Working Party Opinion 05/2014, p. 8 f. See also Cannataci (2009), p. 9; Solove (2002), p. 1152 f.
1105 Feiler (2010), p. 11.
1106 Köpsell/Pfitzmann (2003), p. 15 f.; Pocs (2011), p. 164.

can identify a person very accurately without his or her knowledge,[1107] and the interconnectivity of databases allow access to a wealth of information on the person just identified.

This trend of ubiquitous identification may be connected to higher demands of data protection and privacy. *Köpsell and Pfitzmann* propose the interpretation that in the end, data protection is a necessary development in answer to the process of de-anonymization in digital society.[1108] Effective data protection, encryption, and anonymity allows data subjects to take a step back into the anonymous society existing before the ubiquitous processing of personal data.[1109] Protecting one's personal data thus also means protecting oneself from identification by others, and allows the data subject to enjoy a measure of anonymity in his or her day-to-day life.[1110] In this context, *Köpsell and Pfitzmann* also note that the term 'anonymity' has gained a much more positive connotation today compared to what it had in the 1980s. Although at that time, there was a much higher level of anonymity in society, the term generally carried negative connotations. After the turn of the century, when the general population became more aware of the erosion of this general anonymity through modern data processing techniques, and a portion of the population began to seek a return to more privacy, the term *anonymity* underwent a change and gained a more positive connotation.[1111]

*Rittgen* claims that anonymity is generally not a goal in itself towards which people work, and that there is almost always another reason behind a person wishing to protect his or her anonymity, other than simply not wanting to be identified.[1112] In part for this reason, a person who values his privacy and aims at anonymity, particularly in an online context, may face the imputation that he has "something to hide".[1113] It is easy to presuppose a negative reason for the wish for anonymity, for example in order to hide oneself from persecution for a crime, or to be able to break social conventions without facing repercussions.

*Maras* describes anonymity similarly but rather positively:

1107 Monteleone (2012), p. 5 f.
1108 Köpsell/Pfitzmann (2003), p. 16. See also Worms/Gusy (2012), p. 92 f.
1109 Nicoll (2003), p. 109 f.; Karg (2013), p. 76 f. See also Swire (2012), p. 203 f.
1110 See also Brandeis/Warren (1890), p. 196 on the desirability of a high degree of privacy.
1111 Köpsell/Pfitzmann (2003), p. 16.
1112 Rittgen (2012), p. 10.
1113 Fundamentally Solove (2007), p. 403 ff. See also Simmel (1906), p. 463 f.; Edwards/Howells (2003), p. 213 f.; Maras (2012), p. 69.

> "As such, anonymity refers to the ability of individuals to conduct their lives without making their activities known to others. Anonymity allows individuals to avoid justifying themselves and their personal preferences (religious, political, and sexual) in the face of scrutiny and allows them to arrange their lives in ways that may differ from those exercising disciplinary power or in the case of sexual preferences (maybe even political views) allowing them to differ from social expectations (possible conservative views frowning on bisexuality, transsexuality or homosexuality). In view of that there exist perfectly legitimate reasons for wanting to remain anonymous. Another example may be that individuals may want to present some idea publicly but do not want everyone to identify them, even authorities, especially if they are expressing unpopular views."[1114]

Similarly, *Diderot and d'Alembert*, whose 1751 definition of anonymity in the first instance only covered authors of literary works, quote *Baillet* with several reasons for the preference for anonymity.

> "'Among the authors', says M. Baillet, 'some suppress their names in order to avoid the embarrassment or confusion of having written badly, or having chosen a bad subject; the others, to avoid the recompense or reward which might be paid to them from their labour: some for the fear of exposing themselves to the public, and of being talked of too much; some for a motive of pure humility, trying to make themselves useful to the public without being known; the others finally for indifference and contempt of that vain reputation which comes from writing, because they consider it a baseness, and a sort of dishonour […], to pass for authors, as has sometimes been done by royalty, publishing their own work under the name of their servants.' Jugem. des Savans, tome I."[1115]



However, the increased awareness of the erosion of privacy is slowly changing this perception, and there is a large part of the population who object to their personal data being processed and their privacy being intruded upon.[1116] This is evidenced for example by the large amount of attention generated by topics related to privacy and data protection in the media. An increased awareness of

1114 Maras (2012), p. 78.
1115 Diderot/d'Alembert (2016) s.v. "Anonymous".
1116 Froomkin (2003), p. 45.

the negative consequences of massive data collections, personality profiles,[1117] and other intrusions into a person's privacy may lead individuals to exercise their right to data protection and to be more careful in sharing their data.[1118] The awareness of potentially being under constant surveillance, particularly in an online context through tracking, cookies, malware and other tools,[1119] seems to have awoken in many individuals a desire to protect themselves from such intrusions. The most effective means for such protection is anonymity or pseudonymity, depending on the circumstances of the individual case.[1120]

Protecting one's privacy is a valid interest, supported by no less a principle than the human rights to privacy and data protection.[1121] Therefore, an individual should always be encouraged and supported in protecting these rights, and to exercise his rights to privacy and data protection. As individuals may value the right to privacy differently, some individuals may choose for higher protection, and others for lesser protection. The important issue is that a meaningful choice exists, that the option for anonymity is available for those who wish to choose it.[1122]

### iii. Different Types of Pseudonymity

Anonymity, however, may not always be desirable in human interaction, and may prove impracticable where contact is to be maintained for some time. Therefore, a person may choose to use a pseudonym rather than operating anonymously.[1123] In the same way, data sets can also be pseudonymised rather than anonymised in order to make the link between personal data and the data subject's identity less obvious. The Article 29 Working Party defines the act of pseudonymisation as "replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymisation when used alone will not result in an anonymous dataset."[1124]

1117 See in this context also the census decision, BVerfG, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 [1983]. See also Hornung/Schnabel (2009a), p. 87; Baum (2013), p. 583.
1118 Rittgen (2012), p. 10. See also Simitis (1998), p. 2477.
1119 Webster (2012), p. 18 f.
1120 Froomkin (2003), p. 45.
1121 See, in this context, also Simmel (1906), p. 462.
1122 Rittgen (2012), p. 10. Note that this is not the case in the Anti-money laundering Directive. See Chapter II above for additional details.
1123 Edwards/Howells (2003), p. 213.
1124 Article 29 Working Party Opinion 05/2014, p. 20. See also Hammer/Knopp (2015), p. 507.

Pseudonymity usually contains a much larger risk for identification than anonymity, as the collection of information and establishment of links is much easier if an active pseudonym is used. This is the reason why pseudonymous data is generally considered personal data within the scope of the GDPR.[1125] Yet, a pseudonym may provide a simple though effective barrier behind which an individual can hide their identity: While it is not impossible to discover the identity of the user of the pseudonym, the effort of establishing links may already deter a large number of attackers from attempting to uncover it.[1126] There are several different cases of pseudonymity, which offer a different degree of protection of one's identity. *Köpsell and Pfitzmann* have identified five different types of pseudonyms, which they describe as follows, ordered from the weakest protection of one's identity to the strongest.

In the first case, there are so-called *personal pseudonyms* ("Personenpseudonym"). A personal pseudonym is simply a different name used by a person. The risk of identification is very high,[1127] as this pseudonym is used in so many different contexts that the sum of these may allow the establishment of a link between the pseudonym and the identity of a person. This type of pseudonym is not usually used to hide one's identity from society.[1128]



Furthermore, there is a second group of pseudonyms which may be called *role pseudonyms* ("Rollenpseudonym"). In this case, a person chooses another name for him- or herself to use in only a specific context. To quote an example from a short story by *Thomas De Quincey*: "Chance ordered otherwise. Or, as a Frenchman says with eloquent ingenuity, in connection with this story, 'Chance is but the pseudonyme of God for those particular cases which he does not subscribe openly with his own sign manual.'"[1129] For instance, an author may publish her books under a pseudonym, or a singer might be known by his stage name. The risk of identification depends on the context. A writer using a pseudonym may be in a better position than a singer, as the former needn't necessarily appear in

1125 Article 29 Working Party Opinion 05/2014, p. 10. Pseudonymous data relates to an indirectly identifiable person.
1126 Article 29 Working Party Opinion 05/2014, p. 20. See, in this context, also Simmel (1906), p. 462 f.; Froomkin (2003), p. 9 f.
1127 Köpsell/Pfitzmann (2003), p. 18.
1128 Where an individual is constantly using a personal pseudonym, it may be argued that he or she is directly identifiable just as when using one's real name.
1129 De Quincey (1854), p. 128 f. *Sic.* Depending on the specific context, this illustration may also be classified as a role pseudonym.

public, whereas public appearances are an important part of the latter's profession. However, if the role pseudonym of a writer is used in several books, an attacker may be in the position to collect enough evidence to connect the dots and link the pseudonym to the real identity of the writer.[1130] A famous example for a role pseudonym might be that of *Satoshi Nakamoto*, who used this pseudonym when setting up Bitcoin, and communicated with other developers using this pseudonym. *Nakamoto* is until today successfully concealing his, her, or their real identity.[1131]

In the third place, there are *relationship pseudonyms* ("Beziehungspseudonym"). A relationship pseudonym indicates a pseudonym which is used only for one specific partner in communication. If more than one communication partners exist, the pseudonym holder will use a different pseudonym for each partner. Thus, whenever a pseudonym holder communicates with a specific partner, he uses a particular pseudonym. The content of the communication is not of consequence: in the case of a relationship pseudonym the same pseudonym may be used for private as well as business communications with a given partner.[1132] The risk of identification is increased by this last circumstance: if a communication partner can gather enough information about a person using a relationship pseudonym, there is always a risk of identification. Especially the information contained in private conversation can often provide links to the person's real identity.

The fourth type of pseudonym is a hybrid of role and relationship pseudonyms, and thus also named *role relationship pseudonym* ("Rollenbeziehungspseudonym"). In this case, a different pseudonym is used for each communication partner, just as in a regular relationship pseudonym, but if the pseudonym holder communicates with the same partner in different contexts, a different pseudonym is used for each of those contexts.[1133] Thus, if a pseudonym holder shares, for instance, both private and business communications with the same communication partner, he will use two different pseudonyms in his dealings with this partner: one of which he only uses for business communications with this person, and the other is used for private communication. While using this type of pseudonym offers a greater

1130 Köpsell/Pfitzmann (2003), p. 18.
1131 See *Davis* (2011) for a list of early theories that were developed and abandoned around the identity of Satoshi Nakamoto.
1132 Köpsell/Pfitzmann (2003), p. 18.
1133 Köpsell/Pfitzmann (2003), p. 18.

degree of protection of the pseudonym holder than the previous examples, the risk is still present, and the use of a role relationship pseudonym can be difficult and inconvenient, though tools are available for the use of such pseudonyms in an online context.[1134]

Finally, there are so-called *transaction pseudonyms* ("Transaktionspseudonym"). A transaction pseudonym offers the highest degree of protection from identification, because a pseudonym is used only for a specific transaction and then discarded.[1135] Thus, the information shared by the pseudonym holder pertains only to the transaction in progress and thus offers only a minimum of information that could be used to link the pseudonym to the real identity of the pseudonym holder. A good example for a transaction pseudonym would be a Bitcoin wallet address, if the user uses each address only once, as is recommended.[1136]

## c. Anonymity in the Law

### i. Anonymity as a Right

In many traditions, anonymity is seen as a way to protect the effective practice of freedom of expression. Anonymity thereby allows people to express themselves, and say or do things which are, though perhaps not illegal, not necessarily sanctioned by their environment, society as a whole, or the government.[1137] Anonymity can protect people from discrimination,[1138] threats, harassment, or revenge.[1139] In this way, anonymity is closely connected to the right to privacy, which can also be seen as an enabling right for other human rights, such as the freedom of expression.[1140] Whistle blowers generally rely heavily on anonymity when they share information, because if they do not hide their identities, they are likely to face consequences such as long prison terms or exile. The same is true for dissidents in countries under dictatorial rule, politicians of the opposition, but also people who wish to rebuild a life, such as victims of crime, former criminals

1134 Köpsell/Pfitzmann (2003), p. 19.
1135 Köpsell/Pfitzmann (2003), p. 18.
1136 Nakamoto (2008), p. 6.
1137 Rodriguez (2011), p. 9; Korff (2014), p. 88. See also Diderot/d'Alembert (2016) s.v. "Anonymous". Interestingly, *Diderot* himself was subject to sanctions for publishing his encyclopedia.
1138 See also Korff (2014), p. 90; Schertz (2013), p. 723.
1139 Rodriguez (2011), p. 9.
1140 Korff (2014), p. 88; De Hert (2003), p. 48. See also Grijpink/Prins (2003), p. 255 f.; Karg (2015), p. 520.

after completing a prison term,[1141] or people suffering under or recovering from severe illnesses.[1142] All those people may need to protect themselves and cover aspects of their lives in anonymity in order to live their lives and do their jobs without inviting molestation and offence.

Some countries offer more extensive or more explicit protection for anonymity than others. The Supreme Court of the United States, for example, has held that "Anonymity is a shield from the tyranny of the majority", which "exemplifies the purpose" of the right to free speech, and is therefore protected by the First Amendment, "to protect unpopular individuals from retaliation…at the hand of an intolerant society".[1143]

In Europe, anonymity is generally not as explicitly protected on a constitutional level. A separate right to be anonymous is not generally recognized, though the protection of the individual's privacy is arguably rather strong in Europe compared to other legal traditions.[1144] The national law might, however, make certain provisions for anonymity and pseudonymity on a lower level than on constitutional level. For instance, in Germany, the German Broadcast Media Act (*Telemediengesetz, TMG*)[1145] contains a specific provision on anonymity and pseudonymity in article 13 (4) TMG. According to this provision, the provider of broadcast services must allow users to use services anonymously or pseudonymously, as far as this is technically possible and reasonable.[1146] This provision thus allowed users to protect their identity while using broadcast services. However, the Broadcast Media Act is going to be reviewed in the course of the implementation of the GDPR, and this particular provision may not endure the implementation.[1147]

However, even where such a right to anonymity and pseudonymity is not spelled out explicitly, the right to data protection connects to anonymity. The interest in using information services anonymously or pseudonymously may be seen to be

1141 See Schertz (2013), p. 723.
1142 Rodriguez (2011), p. 9.
1143 United States Supreme Court, *McIntyre v. Ohio Elections Comm'n*, cited in Rodriguez (2011), p. 9. See also Froomkin (2003), p. 16 f.
1144 See Weichert (2007), p. 593 f.
1145 Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBl. I S. 1766) geändert worden ist.
1146 See also Holznagel/Sonntag (2003), p. 133.
1147 Schantz, (2016), p. 1841.

generated to some extent by the principle of data minimization.[1148] According to the data minimization principle, personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5 (1) (c) GDPR). In many cases, a limitation of the collection of data to what is necessary should result in an option for anonymity, and thereby in increased protection.

Similarly, an option to anonymity may in some situations follow from the right to privacy. The theory of spheres was discussed in Chapter V, section (d). The theory of spheres is essentially a model with which the intensity of intrusions into the privacy of individuals can be estimated. The privacy of individuals is split into three spheres: The outer boundary is the public sphere in which the individual is aware of the chance of being observed and overheard by others, and may adapt his or her behaviour accordingly.[1149] The second sphere is the private sphere, in which the individual expects his or her privacy to be respected.[1150] This concerns for instance the individual's own home or correspondence with family and friends. Finally, the intimate sphere is an area of particular privacy. The aspects of an individual's intimate sphere are either completely withdrawn from other persons, or shared only with other individuals with whom a special bond of confidence exists.[1151] Information considered to connect to an individual's intimate sphere is under special protection, as it is often related directly to the human dignity of the data subject.[1152] This connection to human dignity makes the proper protection of the intimate sphere of individuals so imperative. It may be argued, that the protection of the intimate sphere of an individual's privacy would best be achieved by allowing the individual anonymity in such circumstances in which the intimate sphere is engaged.[1153] In many cases, an option for anonymity would therefore be in the interest of the protection of the privacy and dignity of an individual.



It may therefore be stated that in Europe today, there is no universally accepted right to anonymity. An interest in anonymity does, however, often follow from

1148 Schantz, (2016), p. 1841 f. See also Rossum et al. (1995), p. 9; Froomkin (2003), p. 45 f.; Walden (2003), p. 148 f.
1149 Martini (2009), p. 844.
1150 Gurlit (2010), p. 1039.
1151 See in this context Becker/Seubert (2016), p. 74.
1152 Martini (2009), p. 844.
1153 The elaboration of this thought will be continued in section (d) below.

the right to privacy and data protection. Section (d) of this chapter will further elaborate on this approach.

**ii. Pseudonymisation**

Anonymity is the optimal condition in terms of the protection of personal data of a data subject. The data subject is best protected if his or her data is not collected or otherwise processed in the first place. However, such a system is not always possible or even desirable. In such cases, pseudonymisation may often provide the most efficient protection to data subjects.[1154]

In contrast to the terms concerning anonymity, the term 'pseudonymisation' is explicitly defined in article 4 (5) of the GDPR.[1155] According to that definition,

> "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

This definition is further explained in the recitals. Recital 28 GDPR reasons that "the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations." The threshold for pseudonymisation is not too high within the framework of the GDPR. Recital 29 GDPR explicitly speaks of "incentives" that should be created in order to make the use of pseudonyms more attractive to controllers, among which is that

> "measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately."

1154 See also Rossum et al. (1995), p. 11 f.; Knopp (2015), p. 528; Marnau (2016), p. 431 f.
1155 See also Esayas (2015), p. 8; Karg (2015), p. 521 f.

Before the introduction of the GDPR, the concept of creating pseudonyms for data subjects as a measure for data protection was already prevalent in some Member States, and little-used in others.[1156] While the Regulation is therefore adding to the uniformity of the process of pseudonymisation across Europe, the standard of protection is lowered in some countries with the introduction of the standards of the GDPR. In Germany, for instance, pseudonymisation is already a widely-used mechanism for the protection of personal data, although the requirements are high: The data controller has to authorise a third party to the process of pseudonymisation to make sure that the proximity of the original set of data and the derived pseudonymous set does not compromise the protection of the pseudonymisation. The GDPR does not set such high demands to the standard of protection. The standards will therefore, at least in that particular point, lowered with the introduction of the GDPR.[1157]

### iii. Anonymity as Non-Identifiability

As has already been pointed out, data is only considered personal data if it relates to an identified or identifiable person. The absence of such a relation between the data and the identified or identifiable data subject therefore causes the data to lose its nature of "personal" data, and therewith in principle the protection of the GDPR.[1158] That is the reason why anonymity can be a preferred state in data processing from the point of view of the controller or processor, as the obligations of the GDPR to protect this data can then, to a certain degree, be dispensed with.[1159] There are, however, several issues to take into account, namely the question at what point anonymity is achieved, how it is to be achieved, and finally, how anonymity can be maintained over time.



In contrast to pseudonymisation, "anonymization results from processing personal data in order to irreversibly prevent identification."[1160] Therefore, to anonymise data means to process personal data in such a way as to destroy the link between the identifiable person and the data.[1161] That anonymization is an act of processing

1156 Schantz (2016), p. 1843.
1157 Schantz (2016), p. 1843. See also Hammer/Knopp (2015), p. 507; Karg (2015), p. 522. See also Richter (2016b), p. 585.
1158 Other legal safeguards may still apply to the data, see Article 29 Working Party Opinion 05/2014, p. 11.; Wieczorek (2011), p. 477.
1159 Article 29 Working Party Opinion 05/2014, p. 11; Esayas (2015), p. 3.
1160 Article 29 Working Party Opinion 05/2014, p. 3. See Wigoutschnigg (2012), p. 516 f. for possible methods for anonymization. See also Hon/Millard/Walden (2011), p. 214 f.
1161 Article 29 Working Party Opinion 05/2014, p. 8. See also Esayas (2015), p. 4 f.; Buchmann (2015), p. 511.

of personal data is particularly important because as an act of processing, the legal safeguards of applicable to the processing of data are applicable to the anonymization of data as well.[1162]

It must again be emphasized that the concept of anonymity goes beyond the mere absence of the real name of the data subject.[1163] Where a set of personal data is altered simply by omission of the name of the data subject, the data subject can usually still be easily identifiable due to the set of attributes other than a name contained in the dataset: "In many cases it can be as easy to identify an individual in a pseudonymised dataset as with the original data."[1164] Instead, anonymity should be absolute in the sense that identifiability of the data subject is excluded as far as possible. This is supported by the text of the Regulation, when in recital 26 GDPR it states that "[t]he principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

When a person is identifiable is an important and difficult thing to determine.[1165] The Regulation defines the term "identifiable natural person" as a person

> "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".[1166]

The recitals further clarify this definition. As recital 26 GDPR states,

> "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably

1162 Article 29 Working Party Opinion 05/2014, p. 7. See also Hon/Millard/Walden (2011), p. 214.
1163 Article 29 Working Party Opinion 05/2014, p. 21; Grijpink/Prins (2003), p. 254 f.
1164 Article 29 Working Party Opinion 05/2014, p. 21.
1165 Knopp (2015), p. 529; Marnau (2016), p. 429 f.
1166 Article 4 (1) GDPR.

> likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."[1167]

This definition prompts several subsequent questions, which are not all conclusively answered by the text of the GDPR. One important question is raised by the term 'reasonable' itself.[1168] Of course, for different entities or persons, different means are reasonable to be used. The dual level of the controller and 'another person' muddies the waters still further. The means reasonably likely to be used by a specific data controller might be to a certain degree definable. The means reasonably likely to be used by 'another person' less so,[1169] considering that this would depend very much on the type of entity and the resources available to that entity both at that point in time and in the future. It is then surprising, *Schantz* justifiably goes so far as to call it "irritating",[1170] that the legislator did not clarify this point further.

A positive development is the explicit mention of the "technological developments",[1171] which is understood to mean that account must be taken of technological progress, which makes information easier to obtain, faster to process, and simpler to link to other information.[1172] Particularly the development of Big Data and Open Data databases prompts the availability of tremendous amounts of data,[1173] making the future possibilities of identification simply impossible to gauge ex ante.[1174] The Article 29 Working Party also emphasises this point: "Therefore, it is neither possible nor useful to provide an exhaustive enumeration of circumstances when identification is no longer possible."[1175] This increased ease of connecting the dots makes it also easier to identify a person previously considered anonymous, and therefore a safeguard regarding possible future development is absolutely



1167 See also Article 29 Working Party Opinion 05/2014, p. 9; Walden (2003), p. 149 f.; Wieczorek (2011), p. 478.
1168 Esayas (2015), p. 2.
1169 Schantz (2016), p. 1843.
1170 Schantz (2016), p. 1843.
1171 Recital 26 of the GDPR.
1172 Schantz (2016), 1843. See also Nicoll (2003), p. 99; Kemp (2014), p. 482; Richter (2016b), p. 582.
1173 Weichert (2014), p. 833; Raabe/Wagner (2016), p. 434 f.; Sarunski (2016), p. 425; Goldschmidt/Bunk (2016), p. 463; Custers/Uršič (2016), p. 10 ff.
1174 Oostveen (2016), p. 306 ff.; Custers/Uršič (2016), p. 10 ff.
1175 Article 29 Working Party Opinion 05/2014, p. 8. See also Hammer/Knopp (2015), p. 505.

necessary. That the existing safeguards were not strengthened into a meaningful protection in the GDPR is then rather disappointing.[1176]

**iv. Potential Identifiability**

The aforementioned technological progress is by far the biggest threat in the context of anonymous data. It should also be mentioned that anonymization, while in principle set out to be irreversible, is not a guarantee for the protection of the identity of the data subject. As the Article 29 Working Party points out,

> "on the one hand, anonymization and re-identification are active fields of research and new discoveries are regularly published, and on the other hand even anonymised data, like statistics, may be used to enrich existing profiles of individuals, thus creating new data protection issues."[1177]

Anonymous data is therefore in principle not personal data within the scope of the GDPR, but there is always some residual risk to the original data subjects which should not be underestimated.

This residual risk is the main parameter that should be applied in order to assess whether personal data was successfully anonymised and may therefore really be treated as anonymous, rather than as data relating to an identifiable person. Data controllers must therefore choose carefully the means and strategies employed in order to anonymise data.[1178] As the Article 29 Working Party points out, "data controllers should focus on the concrete means that would be necessary to reverse the anonymization technique, notably regarding the cost and the know-how needed to implement those means and the assessment of their likelihood and severity."[1179]

The cost and know-how needed to apply de-anonymization techniques are a difficult factor to assess, particularly as technologies which could potentially be used can sometimes advance rapidly.[1180] In addition, new data sets are

1176 See also section (d) below.
1177 Article 29 Working Party Opinion 05/2014, p. 4. See also Korff (2014), p. 31; Richter (2015), p. 738; Roßnagel/Nebel (2015), p. 459.
1178 Hon/Millard/Walden (2011), p. 214 f.
1179 Article 29 Working Party Opinion 05/2014, p. 8 f.
1180 This is exemplified for instance by the rather sudden ubiquity of face recognition tools. See Monteleone (2012), p. 5 f.; Walden (2003), p. 149 f.

continuously published and made available, particularly in the context of Big Data and Open Data, increasing the risk of identifying a person by linking different data sets.[1181] Therefore, it can be said that "An effective anonymization solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset."[1182] However, it is evident that such a solution would also severely limit the options of the data controller as to how to use the data, as each processing operation would have to be assessed as to the risk of de-anonymization it brings with it.

The risk of de-anonymization also concerns third parties who receive an already anonymised dataset. Those third-party controllers can use this data without needing to take account of the provisions of the GDPR as long as the data is indeed reliably anonymised. However, this third-party controller can only rely on the anonymity to a certain extent. The risk of de-anonymization of the data also depends on what additional other datasets the controller has access to, what technical means are available to him, and how the dataset is to be used. These factors may well lead to a risk of re-identification, in which case the controller must act in accordance with the provisions of the GDPR when processing this data.[1183]



Finally, it should be pointed out that even where data is properly anonymised and therefore falls outside of the scope of the GDPR, the right to privacy might still apply to those datasets. As the Article 29 Working party points out, "as such, even though data protection laws may no longer apply to this type of data, the use made of datasets anonymised and released for use by third parties may give rise to a loss of privacy."[1184] This note is particularly relevant in the context of profiling,[1185] where anonymised datasets and statistics are frequently used to enrich profiles.

1181 Article 29 Working Party Opinion 05/2014, p. 9; Esayas (2015), p. 6 f.; Pordesch/Steidle (2015), p. 539; Rubinstein (2013), p. 76 f.; Oostveen (2016), p. 306 ff.; Custers/Uršič (2016), p. 9 ff.
1182 Article 29 Working Party Opinion 05/2014, p. 9. See also Tschorsch/Scheuermann (2016), p. 2105.
1183 Article 29 Working Party Opinion 05/2014, p. 10. See also Richter (2015), p. 738 f.
1184 Article 29 Working Party Opinion 05/2014, p. 11.
1185 See in this context also Bou-Habib (2011), p. 34; Hammer/Knopp (2015), p. 505; Richter (2016b), p. 582 f.

### v. A Limit to Anonymity

It has thus been established that anonymity is a desirable tool in order to protect one's privacy and identity. However, it should be emphasised that anonymity is naturally not desirable from the perspective of law enforcement agencies.[1186] *Allen* calls anonymity "the core challenge" faced by law enforcement agencies in their fight against (online) criminal activity.[1187] Just as law-abiding individuals have a legitimate interest in protecting their identities, personal data and privacy through anonymity, law enforcement agencies have a legitimate interest in uncovering the identity of malicious users and offenders. The challenge is to effectively protect both interests.[1188]

This challenge is widely recognised. In the words of *Allen,* discussing an online context, "Law enforcement leaders embrace the broadest possible privacy protections for individuals, but emphasise that absolute internet anonymity is a prescription for catastrophe."[1189] Finding the balance is a question of proportionality, which is also the subject of the following chapter.

### vi. Anonymity in the Anti-Money Laundering Directive

One of the areas where an option to anonymity is continually limited is financial transactions. It is considered that anonymity is a major obstacle to efficient investigations into money laundering and particularly the predicate offences to money laundering.[1190] The projected benefit of a limit to anonymity in financial transactions is that all transactions become visible to law enforcement authorities: If law enforcement authorities are in a position to be able to trace all transactions from an identified sender to an identified recipient, activity such as the provision of illegal goods and services, corruption, and tax evasion or fraud woud become significantly more difficult.[1191] It is hoped that this difficulty would deter perpetrators from engaging in such activity. The Anti-money laundering Directive

1186 Carr (2003), p. 193. See also Maras (2012), p. 77; Worms/Gusy (2012), p. 92 f.
1187 Allen (2013), p. 88. See also Leith (2006), p. 124 ff.; Rossum et al. (1995), p. 18 f.; Froomkin (2003), p. 7 f.
1188 See also the third concern discussed in Chapter IX below.
1189 Allen (2013), p. 88.
1190 See for background information for example European Economic and Social Committee 13666/16, p. 6, 8. Critical Sorel (2003), p. 376; Schmidt/Ruckes (2017), p. 473 ff.; Bilsdorfer (2017), p. 1525 ff.
1191 Gouvin (2003), p. 969; Zentes/Wybitul (2011), p. 92.

is one instrument in which the lawmaker is taking steps to realise such a scenario of full identification and traceability.

The Anti-money laundering Directive is an instrument which emphasises identification of all customers of obliged entities. The Directive only once explicitly touches upon anonymity, and only in order to place an absolute ban on anonymous accounts and passbooks. In article 10 (1) 4AMLD, the Anti-money laundering Directive demands that "Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks." Therefore, anonymity as an option for increased privacy in financial transactions is ruled out whenever the customer has a long-term business relationship, an account, with a credit institutions or financial institutions.

Pseudonymisation as a safeguard for increased protection of the identity and the personal data of the data subject is also to a certain extent ruled out by the Anti-money laundering Directive, or rather, it is made very impracticable to use in some contexts. Each obliged entity is under the obligation to identify each of their customers (article 13 (1) (a) 4AMLD). This identification is naturally to be carried out by means of an official document, establishing the full identity of the customer. Pseudonymisation is therefore only used for security reasons, particularly while transmitting data, in order to shield data from an outside attacker.[1192] When the recipient of the data is the FIU in the context of a suspicious transactions report, pseudonymisation is naturally ruled out.



Finally, anonymization of stored data is again excluded by article 40 4AMLD, which obliges all obliged entities to retain information on the identity of their customers for 5 years after the end of the business relationship. The transaction record of each customer also needs to be retained under the rules of the same provision, and thus continues to be connected to the identity of the customer.

In effect, the principle of data minimization is therefore set entirely aside by the terms of the Anti-money laundering Directive for the field of financial transactions.

1192 Article 29 Working Party Opinion 05/2014, p. 21. See also Amendola/Kraus (2015), p. 12 ff.; Grudzien (2015), p. 7 f.

## d. The Unidentified Data Subject

It was argued in section (b) above, that anonymity is in many cases a legitimate interest of individuals. Anonymity is a benefit from the perspective of the right to data protection, as naturally, an individual is best protected where data is anonymous. Furhtermore, anonymity may be demanded of a controller by the principle of data protection. Similarly, the right to privacy may be best protected where the individual is anonymous. This is particularly the case where the intimate sphere of an individual's privacy is concerned, where anonymity is especially desirable.

However, in section (c) of this chapter, it was shown that anonymity is singularly difficult to achieve. The mass of information collected and available on identified individuals leads to a situation in which the possibility that prima facie anonymous information can be linked to an identified or identifiable individual after all. The many instances in which an individual is identified therefore prevent individuals from using an option from anonymity even where it is in their legitimate interest to do so.

This section is therefore dedicated to sketching a way out of this difficulty. It will be argued that the individual's rights to data protection and privacy should be strengthened by a right not to be identified.

### i. The Interest in Anonymity

It was argued in Chapter VI above that the identity of an individual must be protected by special safeguards, if not for its own sake then certainly due to its close connection to the rights to privacy and data protection and human dignity. It was argued in section (d) of that chapter that the individual needs protected spaces or spheres in which to develop one's personality and identity. Such spaces can best be protected and fenced off from outside influences by granting the individual anonymity.

This demand is supported by the text of the law as well. Anonymity is a central concept in the GDPR. In the first place, the Regulation only applies to data relating to an identified or identifiable person and therefore in principle does not apply to anonymous data. The identity or identifiability of a person is therefore the main

basis for the scope of the Regulation. Furthermore, anonymity is in line with the principles of data protection, particularly with the principle of data minimisation.

It has also already been argued above in Chapter VI that the identity of a person is not properly protected by the data protection framework. Individuals need privacy and freedom from observation in order to autonomously develop his or her identity and personality.[1193] The protection of spaces in which an individual may be in a position to freely develop his or her personality can best be achieved by providing for anonymity in those spaces. This means on the one hand that individuals should be granted anonymity where this is necessary for the establishment of such a space, and on the other hand, this means that in some circumstances, anonymity must be enforced by prohibiting the registration of identity. This may for instance be relevant in certain cases of processing of sensitive data, which are closely connected to a person's identity.

However, the law fails to protect the identity of individuals by granting or enforcing anonymity. Indeed, the principle of data minimisation clearly points into the direction of anonymity, but this principle is not endowed with any meaningful enforcement mechanisms. Similarly, the right to be forgotten is a step into the right direction,[1194] but it only comes into play when data has already been collected, and perhaps had been processed in different ways for some time. Therefore, this right also does not offer meaningful protection of a person's identity. In addition to the failure of the GDPR to grant such spaces in which an individual may be anonymous, not to mention to enforce anonymity in any circumstances, the remaining spaces in which a data subject may enjoy anonymity are further eroded by other legal provisions.



The Anti-money laundering Directive is one of the legal provisions further diminishing the situations in which an individual may be anonymous. The Directive summarily bans anonymity in accounts and passbooks in article 10 (1) 4AMLD. This provision read in connection with the obligation to identify customers (article 13 4AMLD) effectively rules out the option for anonymity for the customer whenever he or she makes use of the services of an obliged entity.[1195]

1193 Böhme-Neßler (2016), p. 6 f. See for instance the demand for spaces free from surveillance in Martini (2009), p. 841; Maras (2012), p. 74.

1194 See also Jaspers (2012), p. 572 f.; Leutheusser-Schnarrenberger (2015), p. 586 f.

1195 This complete ban on anonymity is the subject of the third concern discussed in detail in Chapter IX below.

**ii. A Holistic Approach to Identification**

While anonymity is a desirable state in terms of privacy and data protection, it has just been shown that anonymity in the sense of non-identifiability is very difficult to achieve.[1196] Even in anonymous datasets, individuals are almost always indirectly identifiable when the dataset in question is combined with other data. The ready availability of datasets and the massive public and private databases,[1197] not to mention the wealth of information made public by individuals themselves, results in a situation where it is almost impossible to rule out that a data subject is identifiable.

It must be emphasised that this great danger of identifiability is the direct result of the frequent identification of individuals. Where information can be linked, there is always the chance that one of the links which can be established will lead to the discovery of the full identity of a data subject.

Indeed, the ubiquity of identification of the data subject, with the knowledge and perhaps consent as well as unbeknownst to and against the will of the data subject, leads to the identification of the data subject in further situations in which the data subject may initially not have expected to be identified. For instance, a data subject may use public transportation and therefore walk through a train station. He or she will expect the quality of anonymity granted by a crowd of people in any moderately sized to large city. This situation would be significantly altered for instance by the proposed installation of surveillance cameras in public spaces which have face recognition features.[1198] The face recognition software may be supplied with biometric information obtained from social media to which the data subject has uploaded a photograph or to which others have uploaded photographs of the data subject, with or even without the data subject's knowledge and consent. The biometric information may also be gathered from government databases, for instance biometric passport pictures which the data subject was under an obligation to provide.

1196 Article 29 Working Party Opinion 05/2014, p. 9; Esayas (2015), p. 6 f.; Pordesch/Steidle (2015), p. 539; Rubinstein (2013), p. 76 f.
1197 Weichert (2014), p. 833; Raabe/Wagner (2016), p. 434 f.; Sarunski (2016), p. 425; Goldschmidt/Bunk (2016), p. 463.
1198 See Monteleone (2012), p. 5 f.

This example illustrates the (increasing) ease with which individuals may be identified. While in some Member States the application of such technologies is hampered by the local interpretation of the rights to privacy and data protection, they are quickly becoming a reality in other Member States to the European Union. Without wishing to engage at this juncture in a discussion of the compatibility of such plans with the rights to privacy and data protection, particularly the principle of purpose limitation and the principle of proportionality, this example serves to show that when identifying information has been collected in one database, this identifying information can easily be used elsewhere. Identity therefore spreads and disperses though the linking of information.

Whenever identity and anonymity are discussed, this spread and dispersal of identity should be kept in mind. One's anonymity in one context is therefore always dependent on the amount and availability of personal data already collected and processed in other contexts and circumstances. It follows that a data subject cannot really achieve anonymity in one context when he or she has been identified or identifiable elsewhere, and that information is available for linking with the anonymous information in question. The proper assessment and implementation of anonymity therefore demands a holistic view of and approach to identity.[1199]



**iii. A Right not to be Identified?**

Such a holistic view of identity highlights the importance of limiting the situations in which a data subject is identified. The less information on the identity of a data subject is collected and otherwise processed in general, the lower the risk that identifying information is made available for linking previously anonymous information to an identified or identifiable person.

However, the GDPR does not impose any substantive limits on the identification of data subjects. The principles of purpose limitation, of data minimisation, and of integrity and confidentiality are potential keys to such a limit,[1200] but as they are not connected to substantive legal consequences and sanctions, they cannot be considered to provide meaningful safeguards. Similarly, the rights of the data

1199 See also Chapter X below. Just as it is argued here that anonymity cannot be achieved by the data subject due to the ubiquity of identification, it will be argued in Chapter X that privacy cannot be guaranteed to the data subject due to the ubiquity of mass surveillance measures.

1200 See in this context for instance Schantz, (2016), p. 1841 f. See also Rossum et al. (1995), p. 9; Froomkin (2003), p. 45 f.; Walden (2003), p. 148 f.

subject do not ensure a person's freedom from being identified. The rights to be forgotten and to restriction of processing apply to personal data already collected, and do not serve as protection from being identified. A right to anonymity is not included in the GDPR.

Indeed, even if the GDPR did grant the right to anonymity in some circumstances, one may reasonably ask the question whether such a right would be practically meaningful at all. In the first place there is the question of enforceability: the right to anonymity would be very difficult to establish and enforce. Moreover, the difficulty of establishing non-identifiability has been demonstrated.[1201]

However, a meaningful protection of a data subject's identity may be established by asserting a right to not be identified in the data protection framework. Such a right would not go quite as far as a right to anonymity, but it would be much easier to apply. The lawmaker would be called upon to identify situations in which the data subject needs not be identified, such as in circumstances where identification is not necessary for the provision of a service, and where the risks resulting from the lack of identifying information are low. This right may therefore for instance be applied in an online context. It may also be applied in the context of the Anti-money laundering Directive in situations in which property of low value is concerned.[1202]

A right not to be identified would have a positive effect on the data subject in several ways. In the first place, the danger of the spread and dispersal of identity would be greatly diminished if the data subject were not identified whenever such identification can be avoided. The data subject would be more in control of the situations in which his or her identity is known to other parties.[1203] Closely connected is the second major positive effect of such a right on the data subject,

1201 See section (c) of this Chapter above. See also Knopp (2015), p. 529; Marnau (2016), p. 429 f.

1202 The Anti-money laundering Directive in some situations operates thresholds from which on customer due diligence obligations must be applied. However, thresholds apply also when they are reached in a series of transactions which appear to be linked. The value of each transaction in this series will of course be below the threshold, but its value is of no consequence. The Directive operates no de minimis rules. See in this context also the first concern discussed in Chapter IX.

1203 This would also be more in line with the right to informational self-determination, which is not as such discussed in this thesis. See for further information for instance Ronnellenfitsch (2009), p. 451 ff.

namely that the benefit to an individual's privacy would potentially be immense. The data subject would be brought into a better position to carve out spaces for him or herself in which he or she may be free to develop his or her personality.

Difficulties may be expected in applying such a right. Certainly in many circumstances, a service provider has a legitimate interest in identifying the data subject. The application of the right not to be identified would therefore to a great extent depend on a proportionality assessment, balancing the interests of the data subject and the service provider. The lawmaker would need to identify indicators for the legitimate interests of each side, and enumerate them in the law in order to serve as instructions for the application for the right. Such instructions for balancing is, however, already included elsewhere in the GDPR.

As an example, the right to be forgotten includes a list of circumstances which must be taken into account on the side of the data subject and on the side of the service provider. The right to be forgotten is established in article 17 GDPR in the following terms:

"Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
    (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
    (d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
    (a) for exercising the right of freedom of expression and information;
    (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
    (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
    (e) for the establishment, exercise or defence of legal claims."

It can be seen that the right to be forgotten is therefore drafted in a dual structure. In the first paragraph, the lawmaker identifies five situations in which the data subject should be granted the right to demand personal data to be deleted. In the third paragraph, the lawmaker balances the interests of the data subject against

legitimate interests of the service provider, by identifying five reasons in which personal data may be retained.

The circumstances in which the data subject may make use of the right to be forgotten are among other things that the data is no longer necessary for the purpose for which it had been collected (article 17 (1) (a) GDPR), and that the data subject revokes consent (article 17 (1) (b) GDPR). The formulation of these two points brings the weakness of the right to be forgotten criticised above back into focus: the right to be forgotten only applies to data already collected and processed by the service provider. Objecting to the collection of personal data in the first place is not an option.

The scope of the right to be forgotten would have to be extended to a point in time before the data subject is identified in the first place. In principle, all the tools necessary to implement such an extension are already there in the GDPR. The situations in which a data subject may request deletion of personal data, and the situations in which the service provider can demonstrate a legitimate interest in retaining data could be applied in a very similar fashion also to a right not to be identified. The case groups of article 17 (1) (a) and (b) GDPR could be applied: in this way, the data subject would be granted the right not to be identified if identification is not absolutely necessary, and when the data subject does not grant consent.



The latter point would be encumbered with all of the difficulties surrounding the concept of consent in other areas of data protection law as well, particularly the question when consent is free and informed.[1204] The problem of consent is not yet solved in data protection legislation, and attempting to solve it here would go beyond the scope of this thesis. The former point concerning the necessity of identification would likely be the most important case group in practice. Limiting the identification of data subjects to situations in which identification is necessary may be an effective limit to comprehensive data processing operations.[1205] In this way, the data subject would not be identified as often anymore, and it may be possible to fence off spaces where the data subject may be unidentified.

1204 See in this context Simitis (1998), p. 2477; Kühling/Martini (2016), p. 451; Roßnagel (2016), p. 563; Buchner (2016), p. 158.
1205 See also the remarks made on proportionality in Chapter VIII below.

Introducing a right not to be identified is not the only way to protect the identity of a data subject. However, it is clear that additional protection is needed, and expanding the existing right to be forgotten to situations before a data subject was first identified may be the simplest and most effective way for such protection. The right to be forgotten is still a very new right, however, and its application by the CJEU and national courts in the coming years will be observed with interest.

## e. Anonymity and Pseudonymity in Financial Transactions

The concept of anonymity is not at all alien to the financial sector. Indeed, as has been discussed earlier, cash is an anonymous means for financial transactions. This section will focus on the anonymity of financial services rather than the anonymity of media of exchange, however. In this way, the financial services provided by the conventional banking sector, virtual currency systems and informal value transfer services will be briefly discussed.

### i. The Conventional Banking Sector

As has been shown above, anonymity has been entirely eroded and outlawed by the Anti-money laundering Directive, allowing no option for the customer to conceal their full identity. Equally absent are options for the customers of operating only on the basis of a pseudonym or a functional identity.[1206]

Administrative sanctions for non-compliance with article 10 4AMLD, i.e. for retaining anonymous passbooks or accounts, include approaches of naming and shaming,[1207] withdrawal of authorizations or licences, temporary occupational bans, and high fines. Article 59 (2) (e) 4AMLD stipulates that Member States must include in the applicable sanctions "maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000." Article 59 (3) 4AMLD then goes on to increase the maximum possible fines as follows:

1206 See also Article 29 Working Party Opinion 14/2011, p. 11.
1207 See also Shasky Calvery (2013), p. 57.

> "Member States shall ensure that, by way of derogation from paragraph 2(e), where the obliged entity concerned is a credit institution or financial institution, the following sanctions can also be applied:
>
> (a) in the case of a legal person, maximum administrative pecuniary sanctions of at least EUR 5 000 000 or 10 % of the total annual turnover according to the latest available accounts approved by the management body; where the obliged entity is a parent undertaking or a subsidiary of a parent undertaking which is required to prepare consolidated financial accounts in accordance with Article 22 of Directive 2013/34/EU, the relevant total annual turnover shall be the total annual turnover or the corresponding type of income in accordance with the relevant accounting Directives according to the last available consolidated accounts approved by the management body of the ultimate parent undertaking;
> (b) in the case of a natural person, maximum administrative pecuniary sanctions of at least EUR 5 000 000, or in the Member States whose currency is not the euro, the corresponding value in the national currency on 25 June 2015."

Such sanctions are rather compelling to obliged entities. Being confronted with any of those sanctions may mean bankruptcy for a smaller business, and a considerable dent in the corporate image of a larger business. These sanctions contribute to the fact that there is no remaining option for the protection of an individual's identity when that individual operates in his or her capacity of a customer of an obliged entity.[1208]

Pseudonymisation, while being largely ruled out as a means for the protection of the customer's privacy, is frequently used as a security measure by the banking sector. The option usually chosen is that of tokenisation. As the Article 29 Working party explains,

> "this technique is typically applied in […] the financial sector to replace card ID numbers by values that have reduced usefulness for an attacker. It is derived from the previous ones being typically based on the application

1208 These sanctions have a rather compelling effect on service providers. See also Froomkin (2003), p. 39.

> of one-way encryption mechanisms or the assignment, through an index function, of a sequence number or a randomly generated number that is not mathematically derived from the original data."[1209]

Therefore, while anonymization is not an option for the banking sector, it should not be forgotten that pseudonyms are used extensively for security purposes. The use of anonymity could potentially increase this security, if such an option were reintroduced.

The right not to be identified would change this situation to some extent. Primarily other obliged entities, such as sellers of high value goods and casinos, do not necessarily themselves have an interest in identifying the data subject. A right not to be identified would therefore be easily applied. The services of a bank, for instance the electronic transfer of funds, may not necessarily be suitable for the application of anonymity. Some limitation of identification may, however, be achieved also where banks are concerned.

If the right not to be identified were to be applied, however, it would clearly clash with the measures of the Anti-money laundering Directive, making an exploration of the limits of the right necessary. The limits would be defined by law, which may list a number of circumstances in which the right may be limited. The primary test of these limists would, however, be the principle of proportionality. The principle of proportionality is the subject of Chapter VIII. Whether a certain measure is in accord with the principle of proportionality is tested in three steps. The first step is the question, whether the measures are suitable to achieve the aim they pursue. In a second step, it is confirmed that the measures do not go beyond what is necessary to achieve the aim in question. The final step is a balancing of the interests involved.

For the services of the conventional banking system, the last two steps would be of particular note. It would have to be ensured that the duty to identify customers does not go beyond what is necessary, and that the interests of customers are properly taken into account.[1210] While a right not to be identified would certainly not apply absolutely, and may even be limited in the banking sector more than in

1209 Article 29 Working Party Opinion 05/2014, p. 21.
1210 See also the first and third concerns discussed in Chapter IX below.

other sectors, it may be argued that a complete ban on anonymity would not be in accord with the principle of proportionality: where the rights of customers are subject to a ban in an entire branch of industry, it may be difficult to argue that the interests of customers are properly balanced against the other interests involved.

Naturally, the discussion of a right not to be identified is hypothetical at this point. However, the limit to the anonymity of data subject must be balanced against the fundamental right to privacy even now. The erosion of anonymity under the Anti-money laundering Directive is the subject of the third concern discussed in Chapter IX below.

**ii. Virtual Currencies**

It has already been pointed out that virtual currencies are often mistakenly linked to anonymity, while they should be correctly classified as pseudonymous.[1211] In the terms of the data protection legislation, users of virtual currencies should correctly be classified as indirectly identifiable data subjects.[1212] The conditions for anonymity in the sense of non-identifiability are not met. In fact, users face a number of factors which put them at risk of their offline identities being exposed.[1213]

The fact that the user needs not use the services of an obliged entity to take part in the virtual currency environment is, however, seen as an anonymity risk by some entities, for instance the FATF.[1214]

> "For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns."[1215]

1211 Rückert (2016), p. 20; Dowd (2014), p. 69. See also Article 29 Working Party Opinion 05/2014, p. 10; Boehm/Pesch (2014), p. 75. See for a 2003 forecast Froomkin (2003), p. 34 ff.
1212 Rückert (2016), p. 20. See also Böhme/Pesch (2017), p. 478.
1213 Murck (2013), p. 100; Rückert (2016), p. 20; Dowd (2014), p. 70.
1214 FATF virtual currencies (2014), p. 9; Allen (2013), p. 84.
1215 FATF virtual currencies (2014), p. 9; See also Rückert (2016), p. 10 ff.

It is true that no obliged entity is charged with the task of monitoring the blockchain and to identify and report suspicious activity in the virtual currency environment itself.[1216] However, it has already been pointed out in Chapter IV that there are several obliged entities connected to the virtual currency environment, who are charged with identifying customers and with monitoring and reporting suspicious activity within their own respective realms. The core of the anonymity risk as feared by the FATF is the fact that no obliged entity is charged with monitoring the blockchain and the system as a whole. However, the blockchain itself and therefore the entire transaction history of the system is of course entirely public. Each transaction is broadcast to the world, including to law enforcement agencies. The difference is only that instead of a full identity, the only identity available to law enforcement agencies in the first instance is the alphanumerical combination that forms the wallet address relating to the public key used for the transaction.[1217]

However, even when information on a user of a virtual currency system cannot be obtained from an obliged entity, there may still be avenues open to law enforcement agencies to learn the identity of a certain user.[1218] Without assessing the legal conditions for such a cooperation at this point, the most useful partners to law enforcement agencies in discovering the identity of users may be internet services providers.[1219] Naturally, the virtual currency environment can only be accessed via the internet, and every device accessing the internet is assigned an IP address. As virtual currency environments are built upon peer-to-peer networks, any user is vulnerable to being identified via his IP address when connecting to the peer-to-peer network. *Tschorsch and Scheuermann* assure us that if one is connected to all peers in the system, "it is possible to learn the IP address of any transaction originator".[1220] Identification of users of peer-to-peer networks using their IP addresses is a standard procedure in the enforcement of intellectual property rights against users of file sharing networks.[1221] The expertise of representatives of

1216 Rückert (2016), p. 10 f.
1217 See also Pordesch/Steidle (2015), p. 538.
1218 See for a more detailed account Murck (2013), p. 100; Dowd (2014), p. 69; Kasiyanto (2016), p. 152 f.
1219 Allen (2013), p. 88 f.
1220 Tschorsch/Scheuermann (2016), p. 2103. See also Möser/Böhme/Breuker (2013), p. 4; Kasiyanto (2016), p. 153 f.
1221 See also Feiler (2010), p. 14; Sorge (2007), p. 104.

right holders in the identification of infringing internet users could be utilized and adapted by law enforcement agencies in a virtual currency setting.[1222]

This possibility illustrates the vulnerability faced by all unprotected users of the internet.[1223] When a user accesses any webpage, and therefore also any websites related to his or her activity on the virtual currency environment, this activity is liable to being tracked, recorded, and cross-referenced by a number of (background) services. Those services are usually provided by private entities other than the official law enforcement authorities.[1224] The Data retention Directive, for instance, obliged internet services providers to keep a record of visited websites of each user for several months, until the Directive was invalidated in 2014.[1225] Providers in several Member States are still bound to record users' connection history by national law.[1226] That information may potentially easily be searched for information relating to virtual currencies, and when a wallet address is found in this way, it can then be linked to an IP address, which can in turn be linked to the real-life identity of the customer of the internet service provider.

Concealing one's IP address online is not very difficult even for internet users with minimal digital literacy, but all strategies used for such concealment come with weaknesses that might be exploited.[1227] For instance, if a user accesses the system using a Tor Client to route access through a set of other users and thereby distancing himself from the transaction, it is possible for an attacker to trigger a protection mechanism in the system which will ban the exit node through which a user routed his connection.[1228] It has also been reported that law enforcement agencies operate several servers used for the Tor system, enabling them to monitor a large amount of traffic on the system.[1229] Other strategies for anonymous access could also be vulnerable. For instance, *Tschorsch and Scheuermann* speak of a manner of fingerprinting the environment of a target on the peer-to-peer system, by which a user could be identified.[1230]

1222 See in this context also Froomkin (2003), p. 45 f.; Spindler (2012), p. 99.
1223 See also Nicoll (2003), p. 101 f.
1224 See in this context also Cannataci (2013), p. 6.
1225 See for a detailed account the following Chapter VIII.
1226 Not all Member States have yet reacted to CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016]. See critique by Korff (2014), p. 117.
1227 Nicoll (2003), p. 104 f.
1228 Tschorsch/Scheuermann (2016), p. 2103. See also Cannataci (2013), p. 10.
1229 Meister (2017).
1230 Tschorsch/Scheuermann (2016), p. 2103.

The linking of a wallet address to a user's identity is facilitated immensely if the user of the virtual currency used the same wallet address for several transactions.[1231] A role pseudonym is significantly weaker in the protection of a person's identity than a transaction pseudonym, as it provides much more information that can serve as a link between the wallet address and the user's identity.[1232] A large number of users and entities even openly state their wallet addresses among their contact details.[1233] A search of social media platforms such as twitter also reveals a large number of wallet addresses, linked to all the other information that can be collected from that person's account. Even where the owner of that account is not identified directly by name, discovering the identity of the owner of such an account will generally not be too difficult for an engaged law enforcement authority. Also, any entity accepting donations in bitcoin must necessarily share its wallet address. In this way, quite a few users of wallet addresses found in the blockchain can be easily identified by anyone. Identifying these users in turn makes the identification of other users easier. All of the information discussed here is potentially useful for linking. Any link to verifiable information increases the chance of being able to identify the target.

Therefore, while parties to a criminal transaction may not necessarily be known, following further earlier and later transactions through the blockchain may eventually lead to a known party,[1234] such as an exchange or an overground marketplace.[1235] Some identifiable information can likely be found with these parties, be it an IP address, an email address, or even a shipping address.

In sum, it should be stated that the virtual currency system is not anonymous, and that with sufficient technical resources at an attacker's command, it is technically possible to identify a large number of users on the network.[1236] This vulnerability of being identified does not only make it possible for law enforcement agencies to connect a virtual currency user to a real-life identity, but makes the user vulnerable to being identified by any other person as well. Keeping one's financial activity hidden from the world at large is, however, a sensible interest, and should

1231 Article 29 Working Party Opinion 05/2014, p. 11 f.; Allen (2013), p. 88 f. See also Feiler (2010), p. 15.
1232 See the discussion of the different types of pseudonyms in this Chapter above.
1233 Dowd (2014), p. 70; Tschorsch/Scheuermann (2016), p. 2107.
1234 Murck (2013), p. 100; Dowd (2014), p. 69; Pesch/Böhme (2017), p. 96.
1235 Luther (2016), p. 399 f.; Oerlemans et al. (2016), p. 77.
1236 See in this context also Meiklejohn et al (2016), p. 92.

be encouraged and facilitated as much as possible. Users will generally protect their identity by taking steps such as using a different wallet address for each transaction, and accessing the system using virtual private networks and other additional anonymizers.[1237] In the words of *Patrick Murck*,

> "The block chain may be so revealing that the problem with Bitcoin is the difficulty law-abiding people have maintaining privacy. Bitcoin mixing services, which are intended to obscure the source of their users' bitcoins, may become popular if the sense of the Bitcoin community is that the flow of bitcoins is being used for excessive or illegitimate surveillance of private financial activity. Incautious behaviour on the part of governments and law enforcement could make the Bitcoin environment harder to work with."[1238]

The question of anonymity and identity in virtual currency systems is therefore far from solved. It can be concluded, however, that virtual currencies are not anonymous. More than that, due to their open architecture and to the fact that the protection of a user's identity depends on so many factors outside of the user's control, the system does not afford more privacy to the average user than the conventional banking system does.



**iii. Informal Value Transfer Systems**

The misconceptions about the anonymity of Hawala are just as numerous, if not even more so, as those existing about virtual currencies.[1239] Just as virtual currencies, Hawala is also not an anonymous system for financial transactions. In principle, hawaladars are bound to the terms of the Anti-money laundering Directive just like any other financial services provider. In principle, any hawaladar is thus obliged to identify each customer, monitor all transactions, and report any suspicious transactions. However, in practice most hawaladars do not strictly adhere to these standards.

1237 See also Pfitzmann/Köpsell (2009), p. 545.
1238 Murck (2013), p. 100. See also Rückert (2016), p. 20; Möser/Böhme/Breuker (2013), p. 5 f.
1239 See for details Chapters III and IV above.

The FATF itself debunks the myth that hawaladars do not keep any records of transactions[1240] in the following clear terms:

> "many Hawala investigations have revealed that hawaladars and similar service providers actually keep detailed records, they maintain manual accounts, ledgers, computerized records or a combination of these. The businesses of some hawaladars are based on small margins of profit, and recording and tracking deposits, payments and transfers is important to their good reputation and efficiency".[1241]

This interest in record-keeping is then also not diminished by the fact that a hawaladar may suspect, know, or even himself be involved in criminal activity. Clearly, hawaladars who "service the criminal market need to keep detailed records in order to keep track of transactions completed through complex settlement methods such as third party payments and trade transactions."[1242] However, while hawaladars generally do keep records, those may not be quite as detailed and in the form and system as demanded by the Anti-money laundering Directive.[1243]

Of course, there are also some hawaladars who are knowingly and deliberately involved in money laundering or terrorist financing operations. Those hawaladars naturally will avoid keeping any such detailed records of compromising transactions, and particularly of the persons involved in such transactions. This is generally achieved by keeping the information recorded to a minimum or in a way not intelligible to anyone else,[1244] using pseudonyms or tokens,[1245] keeping a second, secret book next to the record of legitimate transactions,[1246] or destroying records as soon as possible after the transaction.[1247]

Furthermore, hawaladars whose businesses are not properly licenced may be reluctant to communicate any suspicious transactions and the parties involved in such transactions to the authorities in order to avoid drawing attention to

1240 See also Razavi (2005), p. 279; IMF (2005), p. 18.
1241 FATF Hawala (2013), p. 19.
1242 FATF Hawala (2013), p. 19.
1243 See also Razavy/Haggerty (2009), p. 141.
1244 Soudijn (2015), p. 263; Razavi (2005), p. 279.
1245 Razavi (2005), p. 279; Soudijn (2015), p. 266 f.
1246 Soudijn (2015), p. 264.
1247 Razavi (2005), p. 279.

themselves and their business activities.[1248] The fact that hawaladars are obliged entities under the Anti-money laundering Directive also means that they are vulnerable to penalties for non-compliance as stipulated in the above-mentioned article 59 4AMLD.[1249] Of course, some hawaladars are also interested in avoiding contact with law enforcement authorities because they are involved in transactions which they know or suspect to have a criminal background.[1250]

In sum, the privacy that a customer can achieve when using the Hawala system is potentially much higher than that generally afforded by the conventional banking sector. The use of anonymous cash combined with the absence of compliance with compulsory identification mechanisms and the wide-spread noncompliance with record keeping requirements may allow for nearly anonymous transactions, depending on the internal administration and bookkeeping of the individual hawaladar. It could therefore be said that Hawala allows for more freedom from surveillance compared to the conventional banking system.

## f. Conclusion



Anonymity and pseudonymity are two highly interesting and complex concepts in the context of privacy and identity, as they allow for potentially very effective protection of an individual's identity, privacy, and personal data. Indeed, as has been shown, anonymity, where it is achieved properly, may be the best possible option for comprehensive protection of one's privacy. Where anonymity cannot be realised, pseudonymity might be very useful for an increased level of protection of personal data and privacy. It should therefore be encouraged in service providers of all descriptions to allow customers to use these services anonymously or under a pseudonym.

It has also been shown in this chapter that the GDPR falls short of a meaningful standard of protection of identity and privacy by failing to include safeguards

1248 See the discussion on how hawaladars are covered by the anti-money laundering rules in Chapter IV above.
1249 The penalties for non-compliance with the Anti-money laundering Directive are very high and will therefore often deter hawaladars from seeking contact with the authorities for any reason.
1250 Soudijn (2015), p. 262.

against a data subject being identified where such identification is not necessary. One possibility for meaningful protection against such identification would be to extending the scope of the right to be forgotten to earlier points in time, expanding the right into a right not to be identified. By applying the same safeguards of the right to be forgotten to a right not to be identified, the legitimate interest of the data subject in proper protection of privacy would be safeguarded.

However, not only does the GDPR not include such a right, other laws also actively counteract the interest of the data subject in not being identified, as is evidenced by the terms of the Anti-money laundering Directive.[1251] The Directive indeed outlaws anonymity outright and explicitly. For the (compliant) conventional banking sector, this has led to a situation in which the customer must be fully identified in order to be granted access to the services provided by this sector. A customer insisting or depending on the protection of his or her identity by anonymity may find the services of obliged entities entirely inaccessible.

This inaccessibility of the conventional banking sector is, however, the situation in which alternative systems for financial transactions may become indispensable to individual customers. Both virtual currencies and the Hawala system can remain accessible to users even if those users have not been formally identified by any other obliged entity. Virtual currencies are most easily accessed using exchanges, but these can be circumvented with relative ease, thereby avoiding the services of an obliged entity. Hawaladars are themselves in principle obliged entities, but as has been seen in this and in the previous chapters, hawaladars often do not comply with the formalities attached to their status as obliged entity.

While such an option for increased anonymity is certainly attractive for users resolved to abuse these financial services for criminal transactions, certainly not all individuals interested in protecting their identity, privacy, and personal data have such criminal intent. An individual's wish to protect these assets is, indeed, a sensible one, and more respect for this wish on the part of the lawmaker would perhaps be creditable.

The points made in this chapter will be expanded in the following Chapters IX and X. The erosion of anonymity by the provisions in the Anti-money laundering

1251 See also Article 29 Working Party Opinion 14/2011, p. 7.

Directive is the subject of the third concern discussed in Chapter IX. The comprehensive identification of data subjects under the Directive is furthermore an underlying criticism of the Directive which comes into play in the overall proportionality assessment and which should be kept in mind across all seventeen concerns.

Furthermore, it has been shown that the approach to identification of data subjects would benefit from a more holistic approach. It was argued that the ubiquity of identification of data subjects make it nearly impossible for individuals to carve out spaces for themselves in which they are anonymous. This holistic view of identification is directly related to the holistic approach to privacy, which will be argued in Chapter X.

# Chapter VIII

## The Principle of Proportionality

## Outline:

a. Introduction
b. The Principle of Proportionality under the ECHR
    i. The European Convention on Human Rights
    ii. The Proportionality Test as Applied by the ECtHR
    iii. Margin of Appreciation
c. Case Law of the ECtHR
    i. Early Cases on the Proportionality of Surveillance Measures
    ii. Personal Data Stored in Secret Police Files
    iii. Taxation and Financial Data
    iv. Personal Data and New Technologies
    v. Most Recent Case Law: *Zakharov v. Russia*
    vi. Summary
d. Proportionality in European Union Law
    i. The Charter of Fundamental Rights of the European Union
    ii. Proportionality in the Law-making Procedure
    iii. The Proportionality Test as applied by the CJEU
    iv. Margin of Appreciation and Judicial Restraint
    v. Suitability of a Measure
e. Necessity and Proportionality in the Case Law of the CJEU
    i. Interferences with the Rights to Privacy and Data Protection
    ii. Early Cases: *Rechnungshof* and *Lindqvist*
    iii. The Right to Privacy and the Interests of Copyright Holders
    iv. Information on the Balancing of Interests
    v. Strengthened Protection of the Right to Privacy: *Digital Rights Ireland* and *Tele2 Sverige*
    vi. Privacy and Individual Interests: *Google Spain*
    vii. International Exchange of Data: *Schrems* and *Passenger Name Records*
    viii. Summary
f. Conclusion

## a. Introduction

At the core of this thesis lies the conflict between the anti-money laundering measures and the rights to privacy and data protection of the individual. Anti-money laundering measures are applied in order to prevent and investigate into the crimes of money laundering and terrorist financing, and the fight against crime is considered an objective in the public interest which the lawmaker legitimately pursues.[1252] The rights to privacy and data protection are human rights, the protection of which is equally in the public interest. The conflict lies in the fact that the one interest limits the other: on the one hand, the rights to privacy and data protection are limited by the extensive data processing measures involved in anti-money laundering; on the other hand, the anti-money laundering measures are limited in extent by the rights to privacy and data protection. The two interests must therefore be balanced by the lawmaker in order to ensure that each interest can be protected to the greatest possible extent. This balancing act is governed by the principle of proportionality.

In the words of *Walter van Gerven*, "Proportionality is a tool to balance conflicting values in order to reconcile them as much as possible in practice."[1253] This principle is of overwhelming importance particularly in the area of human rights, as any limitation of a human right can only be accepted if the limitation is made in favour of a measure which, very simply put, serves a legitimate public interest, and which does not go beyond what is necessary in order to reach the pursued objective.[1254] When a measure goes beyond what is necessary, it is generally not in accord with the principle of proportionality and therefore will be invalidated by the courts when it is challenged.

The principle of proportionality is a principle primarily applied by the lawmaker, and reviewed by Courts, particularly the CJEU and the ECtHR, which both apply a flexible proportionality test. Other instances also apply a proportionality test,[1255] but the case law of these two courts is particularly authoritative in this context,[1256]

1252 See for more information and critique Chapter IX below.
1253 Gerven (1999), p. 51. See for background also Holaind (1899), p. 23 ff.; Bentham (1907), p. 127 ff.
1254 See also Stammler in Hinneberg (ed.) (1906), p. 505 f.; Barak (2013), p. 252 ff.
1255 Gerven (1999), p. 44 ff.; Waldron (2003), p. 198.
1256 That is, the context of European human rights. As the subject of this thesis is the European anti-money laundering legislation, the human rights instruments and case law is

as they can review the application of the principle of proportionality by other entities and remedy offences against it. Their case law with malleable definitions of the principle of proportionality is the basis on which the proportionality of other measures is assessed.

However, as will be seen, the notion that a measure is only proportionate when it serves a legitimate public interest and does not go beyond what is necessary to achieve its objective, is a very simplified concept of proportionality. In reality, the proportionality tests applied by the CJEU and the ECtHR are much more complex and varied than that. This chapter is therefore intended to give an overview over the content and significance of this principle in the system of European law, and the development of the application of this principle by both the CJEU and the ECtHR in their respective realms. While particularly the discussion of the case law can naturally only consider a selection of the extensive case law of the two Courts, the selection has been made so as to include case law with a connection to the right to privacy and data protection. This way, while the proportionality test applied by the Courts is anything but set in stone, a good understanding of the content of this principle can be gained from the following sections.

This chapter is of great relevance to the main research question, which concerns the proportionality of the anti-money laundering legislation. It will therefore create the basis upon which the proportionality of that legislation will be assessed. The application of the principle of proportionality to the anti-money laundering measures will take place in the following Chapter IX.

This chapter is organised in a dual structure, because the two legal instruments of the Charter and the ECHR lay at the core of the discussion. After this introduction, therefore, the principle of proportionality in the regime of the ECHR will be examined (section b), and supplemented by a discussion of case law of the ECtHR (c). In the following section (d), the notion of the principle of proportionality applied within the European Union will be examined, and then the application of the balancing act carried out by the CJEU in judging the necessity of a measure will be traced (section

applied. On the European level, the Charter of Fundamental Rights and the applicable case law by the CJEU as well as the European Convention of Human Rights and the case law by the ECtHR are authoritative.

e). The case law to be examined is limited to cases concerning privacy and data protection, and is grouped according to subject matter and context.

## b. The Principle of Proportionality under the ECHR

### i. The European Convention on Human Rights

The realm of the Council of Europe, which is with its 47 Member States an undertaking even larger in terms of territorial scope than the European Union, covers almost the entire European continent. All European countries are Member States to the Council of Europe, with three exceptions. Belarus is not a Member, but a candidate for accession; the Vatican is not a Member, though the Holy See is an observer; Kosovo is not a Member, and her still uncertain status in international law at present prevents it from becoming a Member State.[1257] On and beyond the geographical borders of Europe, the territory of the Council of Europe also includes Russia, Turkey, and the three Caucasus States.

All Member States of the European Union are at the same time Member States of the Council of Europe, and must therefore comply with the European Union legislation as well as with the European Charter of Human Rights (ECHR) of 1950, the most important achievement of the Council of Europe.[1258] The ECHR is closely connected to the Charter. Not only is the Charter to a large degree based on the ECHR and the case law of the ECtHR, but does it expressly consider the standards of the ECHR the standard below which the protection afforded by the Charter must not sink (Article 52 (3) of the Charter).[1259]



Proportionality is a very important topic in the application of the ECHR. In essence, it expresses "that human rights are not absolute and that the exercise of an individual's rights must always be checked by the broader public interest."[1260] The right to respect for private and family rights is thus not absolute. The right to respect for private life is found in article 8 (1) ECHR, which very simply states that

1257 See United Nations Security Council resolution 1244 (S/RES/1244), adopted on 10 June 1999.
1258 Barak (2013), p. 183. See also Schweizer (2009), p. 463 f.
1259 Article 29 Working Party, Opinion 1/2014, p. 4. See also European Commission (1999), p. 20 f.
1260 Kilkelly (2003), p. 31.

"Everyone has the right to respect for his private and family life, his home and his correspondence." This article is at the same time the source of both Articles 7 and 8 of the Charter, which were modelled principally after it.[1261] However, as most human rights, the right to respect for private and family life can be limited under certain circumstances. One of these conditions is that a limitation is "necessary in a democratic society". The conditions for limiting the right to private life follow immediately in the second paragraph of article 8 ECHR, which reads:

> "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In the words of the ECtHR,

> "[T]he Court must determine whether a fair balance was struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights […]. The search for this balance is inherent in the whole of the Convention."[1262]

It could therefore be stated that assessing the proportionality of a given measure is much like a walk on a tightrope: the assessment of proportionality "at its simplest, involves balancing the rights of the individual and the interests of the State."[1263]

**ii. The Proportionality Test as Applied by the ECtHR**

The CJEU and the ECtHR apply different proportionality tests. In contrast to the proportionality test applied by the CJEU as outlined below, the test applied by the ECtHR is considerably less clear-cut. The principle of proportionality in matters concerning the right to respect for private and family life is essentially made up cumulatively of the conditions contained in article 8 (2) ECHR. The crux of the matter, however, is found in that paragraph in the formulation "necessary

1261 Article 29 Working Party, Opinion 1/2014, p. 3.
1262 ECtHR Case of *Sporrong and Lönnroth v. Sweden* [1982], paragraph 69.
1263 Kilkelly (2003), p. 31. See also Waldron (2003), p. 192.

in a democratic society", which the ECtHR initially filled in with the following description:

> "The notion of necessity implies that the interference corresponds to a pressing social need and, in particular that it is proportionate to the legitimate aim pursued".[1264]

As will be seen below, the Court expanded this definition in later case law:

> "An interference will be considered "necessary in a democratic society for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."[1265]

In sum, therefore, the three criteria handled by the ECtHR to determine the legality of an interference with the right to respect for one's private life are (1) that the interference must be in accordance with the law, (2) that the measure must pursue a legitimate aim, and (3) that the interference is necessary in a democratic society.[1266] The final criterion represents the principle of proportionality.[1267]

What the term 'necessary in a democratic society' precisely means, however, is far from clear. The ECtHR is applying different tests to ensure the compliance with this principle. Those can be roughly summarised to mean that the legislation (1) answers a pressing social need and (2) that relevant and sufficient reasons have been given for it, and finally, (3) that sufficient safeguards exist to protect individuals against abuse.

In addition, other considerations are frequently brought up by the Court. In this way, the Court's case law shows that the interference with some rights is much more difficult for the state to justify than an interference with other rights. For instance, the ECtHR's case law shows that the rights of adults to develop their sexual identity cannot be interfered with by the state, unless an interference is

1264 ECtHR Case of *Leander v. Sweden* [1987], paragraph 58.
1265 ECtHR Case of *S. and Marper v. The United Kingdom* [2008], paragraph 101.
1266 Article 29 Working Party, Opinion 1/2014, p. 5. See also Article 29 Working Party, Working Document 1/2016, p. 7 ff.
1267 Schweizer (2009), p. 467.

justified by exceptionally urgent considerations. "Some rights will thus inevitably be afforded more importance than others, making interferences with them very difficult to justify."[1268]

Similarly, there are different types of interferences, some of which will be more acceptable to the Court than others. It is quite obvious that a particularly serious interference with the rights of an individual can only be justified by the most urgent considerations.[1269] Conversely, where the reasons cited to justify an interference are less potent, they can only justify a milder intrusion into the rights of an individual. In this way, the ECtHR applies a similar balancing scale as the CJEU does in its assessment of proportionality in *stricto sensu*.

The text of the ECHR was drafted in 1950, and therefore the contents of the Convention have accompanied and shaped European societies from the post-war period until today. The ECtHR as the authority tasked with the interpretation of the Convention has reflected many changes that occurred within the European society in the past 67 years, among other things, with a dynamic interpretation of the term proportionality. This dynamic interpretation will be traced to some extent in the discussion of the Court's case law, below.

### iii. Margin of Appreciation

It must be emphasised that the Courts are generally cautious in their assessment of the means chosen to achieve a certain aim, because due to the separation of powers, they must not attempt to encroach upon the powers of the legislators.[1270] Therefore, the ECtHR's assessment of the proportionality of a given measure is also marked by restraint on the side of the Court.

> "The concept of the margin of appreciation is that a government's discharge of these responsibilities is essentially a delicate problem of appreciating complex factors and of balancing conflicting considerations of the public interest; and that, once the Commission or the Court is satisfied that the Government's appreciation is at least on the margin of the powers conferred by Article 15, then the interest which the public

1268 Kilkelly (2003), p. 32. See also Schweizer (2009), p. 468.
1269 Kilkelly (2003), p. 32; Bizer (2007b), p. 587.
1270 Craig (1999), p. 102.

> itself has in effective government and in the maintenance of order justifies and requires a decision in favour of the legality of the Government's appreciation."[1271]

In another case, the Court continued to explain this notion in the context of a value judgment made by a Member State concerning public morals.

> "In particular, it is not possible to find in the domestic law of the various Contracting States a uniform European conception of morals. The view taken by their respective laws of the requirements of morals varies from time to time and from place to place, especially in our era which is characterised by a rapid and far-reaching evolution of opinions on the subject. By reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements as well as on the "necessity" of a "restriction" or "penalty" intended to meet them. The Court notes at this juncture that, whilst the adjective "necessary", within the meaning of Article 10 para. 2 (art. 10-2),[1272] is not synonymous with "indispensable" […], neither has it the flexibility of such expressions as "admissible", "ordinary" […], "useful" […], "reasonable" […] or "desirable". Nevertheless, it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in this context."[1273]



Therefore, while the purpose of the proportionality assessment is to assess and review the measures chosen by the legislator, the application of the principle of proportionality by the ECtHR is marked by a great respect for the realm of the legislative.[1274] However, this respect is of course not unlimited. The limits of the margin of appreciation the Court grants to a state depends on the specific

1271 ECtHR Case of *Lawless v. Ireland* (rep.) [PL], (19 December 1959, Series B no. 1) p. 397 (Verbatim record of the hearing on 8 April 1961), quoted in Christoffersen (2009), p. 244. See also McBride (1999), p. 29.
1272 Article 10 ECHR protects the freedom of expression. Footnote added by the author.
1273 ECtHR Case of *Handyside v. the United Kingdom* [1976], paragraph 48. See also Kilkelly (2003), p. 6 f.; Craig (1999), p. 102; Barak (2013), p. 184.
1274 Kilkelly (2003), p. 7; McBride (1999), p. 29.

circumstances of a case and on the rights involved.[1275] To quote an excellent explanation of *Lord Reed*,

> "An assessment of proportionality inevitably involves a value judgment at the stage at which a balance has to be struck between the importance of the objective pursued and the value of the right intruded upon. The principle does not however entitle the courts simply to substitute their own assessment for that of the decision-maker. As I have noted, the intensity of review under EU law and the Convention varies according to the nature of the right at stake and the context in which the interference occurs. Those are not however the only relevant factors. One important factor in relation to the Convention is that the Strasbourg court recognises that it may be less well placed than a national court to decide whether an appropriate balance has been struck in the particular national context. For that reason, in the Convention case law the principle of proportionality is indissolubly linked to the concept of the margin of appreciation. That concept does not apply in the same way at the national level, where the degree of restraint practised by courts in applying the principle of proportionality, and the extent to which they will respect the judgment of the primary decision maker, will depend upon the context, and will in part reflect national traditions and institutional culture."[1276]

Therefore, the application of the principle of proportionality should always be considered to be tempered somewhat by the Court's application of the doctrine of the margin of appreciation. At the same time, it should once again be emphasised that naturally, there are limits to the margin of appreciation enjoyed by governments in designing a legal instrument.

> "Admittedly, the Court has consistently held that the Contracting States have a certain margin of appreciation in assessing the need for interference, but it goes hand in hand with European supervision. The exceptions provided for in paragraph 2 of Article 8 are to be interpreted

1275 Kilkelly (2003), p. 32 f.
1276 Lord Reed in Supreme Court of the United Kingdom, *Bank Mellat v Her Majesty's Treasury* (No. 2) [2013] UKSC 39 (19 June 2013), paragraph 71.

> narrowly […], and the need for them in a given case must be convincingly established […]."[1277]

This above quote sums up the current state of play concerning the doctrine of the margin of appreciation very nicely. It can be said that while states do enjoy a margin of appreciation, any limitation of a right under the Convention must be properly justified and accompanied by appropriate safeguards against abuse.

## c. Case Law of the ECtHR

It was the ECtHR who first developed in its case law the criteria of necessity and proportionality.[1278] In addition, the ECHR and the decisions of the ECtHR are the only international instruments frequently quoted by the CJEU as authoritative.[1279] A look into the case law of the ECtHR is therefore certainly beneficial to gaining a pan-European understanding of the content of the principle of proportionality, particularly of the notion of what is necessary in a democratic society.

The case law is ordered roughly chronologically and by subject matter. In this way, the different groups of cases can best be analysed in connection to one another. The case law of the ECtHR on the proportionality of interferences with the right to respect for private and family life is going to be valuable for the assessment of the proportionality of the measures of the Anti-money laundering Directive. Therefore, the most influential cases in this field are going to be discussed one by one. The analysis of the case law of the ECtHR and the CJEU build the foundation upon which the Anti-money laundering Directive will be assessed.



### i. Early Cases on the Proportionality of Surveillance Measures

One of the earliest ECtHR judgments that are of continued importance is *Klass v. Germany* of 1978.[1280] The case *Klass* concerned a group of five lawyers who challenged German legislation according to which the competent authorities were authorised to monitor their communications. In particular, this law did not contain a right to information for the data subject or an obligation to inform a

1277 ECtHR Case of *Société Colas Est and others v. France* [2002], paragraph 47.
1278 Article 29 Working Party, Opinion 1/2014, p. 5.
1279 Craig/De Búrca (2015), p. 385 f.
1280 ECtHR Case of *Klass and Others v. Germany* [1978].

data subject of a completed surveillance operation, and so the persons monitored may not learn of surveillance measures taken against them.[1281] The ECtHR held unanimously that the provisions challenged in this case did not constitute a breach of article 8 ECHR, but made several interesting observations on the subject in the judgment.

The Court stated in particular that "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."[1282] Following this statement, however, the ECtHR continues with the following observation:

> "As the Delegates observed, the Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years.[1283] Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[1284]

This statement is notable for the fact that, while made by the ECtHR in a judgment in 1978, it might appear in the exact same wording in a judgment of 2017, 39 years after *Klass*.[1285] The Court continues to state that while the government certainly

1281 Boehm/De Hert (2012), p. 5. See also Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 339.
1282 ECtHR Case of *Klass and Others v. Germany* [1978], paragraph 42. See also Rost (2013), p. 86.
1283 See in this context also Maras (2012), p. 66 f. Footnote added by the author.
1284 ECtHR Case of *Klass and Others v. Germany* [1978], paragraph 48. See also Feldman (1999), p. 130 f.; Huber (2007), p. 881 f. See, however, Korff (2014), p. 107 f.
1285 See for example recital 4 of Directive (EU) 2017/541, "The terrorist threat has grown and rapidly evolved in recent years." See also Feldman (1999), p. 131.

enjoys a wide margin of discretion in shaping its policy in this area, that discretion is not limitless: "The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[1286] The Court then continues with an explanation of the proportionality standard that must be observed by the government when introducing such surveillance measures. The Court makes an interesting general statement concerning what it considers to be "necessary in a democratic society".

> "Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2 (art. 8-2), are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention […]. The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[1287]



1286 ECtHR Case of *Klass and Others v. Germany* [1978], paragraph 49. See for the connection between privacy and democracy Böhme-Neßler (2016), p. 5 f. See also Kilkelly (2003), p. 24; Feldman (1999), p. 131; De Hert (2003), p. 48; Barak (2013), p. 214 ff.

1287 ECtHR Case of *Klass and Others v. Germany* [1978], paragraph 55. See also Boehm/De Hert (2012), p. 6; Fraenkel/Hammer (2011), p. 889.

The Court continues to stress that due to the particularly sensitive nature of secret surveillance, the task of reviewing such secret surveillance measures should be entrusted to the judiciary.[1288] The Court finally held that the strong constitutional safeguards applicable to the surveillance measures were sufficient to ensure that the measures did not go beyond what is necessary.

Another relatively early case that should be mentioned in this context is the case *Malone v. the United Kingdom* of 1984.[1289] The difficulties in this case began already with the establishment of an interference, as the authorities simply declined to disclose whether the applicant's telephone had been tapped. Due to the "obscurity and uncertainty" of the legal rules concerning this tapping, the Court found that the interference was not in accordance with the law.[1290] The Court here shed some light on the requirement of foreseeability, which should be highlighted here.

> "Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident […]. Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[1291]

Therefore, the condition of foreseeability means that citizens must, in general terms, be in a position to know about the powers of surveillance of the state and

1288 ECtHR Case of *Klass and Others v. Germany* [1978], paragraph 56. See also Fraenkel/Hammer (2011), p. 889.
1289 ECtHR Case of *Malone v. the United Kingdom* [1984].
1290 ECtHR Case of *Malone v. the United Kingdom* [1984], paragraph 79.
1291 ECtHR Case of *Malone v. the United Kingdom* [1984], paragraph 67. See also Holaind (1899), p. 154 ff.

appreciate their extent properly. The requirement of foreseeability is the more important in this circumstance as the interference with the rights of the individual is potentially very grave, and must therefore be foreseeable and tempered by adequate safeguards. The Court also continues to briefly examine the necessity of the rules.

> "Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2) […]. The Court accepts, for example, the assertion in the Government's White Paper […] that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime". However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole […]. This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse […]."[1292]



As the Court had already found that the rules according to which the surveillance would have been carried out were not in accordance with the law, it did not go into further details on this point. It may, however, be doubted whether a law that made it impossible for an individual to ascertain whether he or she was indeed subject to surveillance would satisfy the Court's ideas of adequate safeguards.[1293]

A further case of the investigation into terrorism and serious crime is *Murray v. the United Kingdom*.[1294] This case is of interest, as it continues the development of the line of case law begun in *Klass*. In this case, the applicants complained of having been arrested and detained, photographed without their consent, and

1292 ECtHR Case of *Malone v. the United Kingdom* [1984], paragraph 81. See also Leith (2006), p. 113.
1293 See also Kilkelly (2003), p. 24 f.
1294 ECtHR Case of *Murray v. the United Kingdom* [1994]. See also McBride (1999), p. 27.

their house being searched. The reason for this treatment was that they had been suspected to be involved in terrorism in Northern Ireland. The Court here carried out the examination of the necessity of the measures taken against the applicants with visible care.

> "The domestic courts held that Mrs Murray was genuinely and honestly suspected of the commission of a terrorist-linked crime […]. The European Court, for its part, has found on the evidence before it that this suspicion could be regarded as reasonable for the purposes of sub-paragraph (c) Article 5 para. 1 […]. The Court accepts that there was in principle a need both for powers of the kind granted by section 14 of the 1978 Act and, in the particular case, to enter and search the home of the Murray family in order to arrest Mrs Murray.
>
> Furthermore, the "conditions of extreme tension", as Lord Griffiths put it in his speech in the House of Lords, under which such arrests in Northern Ireland have to be carried out must be recognised. The Court notes the analysis of Lord Griffiths, when he said […]:
>
> > 'The search cannot be limited solely to looking for the person to be arrested and must also embrace a search whose object is to secure that the arrest should be peaceable. I ... regard it as an entirely reasonable precaution that all the occupants of the house should be asked to assemble in one room. ... It is in everyone's best interest that the arrest is peaceably effected and I am satisfied that the procedures adopted by the Army are sensible, reasonable and designed to bring about the arrest with the minimum of danger and distress to all concerned.'
>
> These are legitimate considerations which go to explain and justify the manner in which the entry into and search of the applicants' home were carried out. The Court does not find that, in relation to any of the applicants, the means employed by the authorities in this regard were disproportionate to the aim pursued.

> Neither can it be regarded as falling outside the legitimate bounds of the process of investigation of terrorist crime for the competent authorities to record and retain basic personal details concerning the arrested person or even other persons present at the time and place of arrest. None of the personal details taken during the search of the family home or during Mrs Murray's stay at the Army centre would appear to have been irrelevant to the procedures of arrest and interrogation […]. Similar conclusions apply to the taking and retention of a photograph of Mrs Murray at the Army centre […]. In this connection too, the Court does not find that the means employed were disproportionate to the aim pursued."[1295]

The Court thus ultimately ruled that the measures taken by the authorities remained within the limits of proportionality; the measures were considered to be necessary in a democratic society. This ruling can be taken as an example of the very wide margin of appreciation the Court will grant to investigating authorities in cases of terrorism and tension.[1296] In its assessment of the proportionality of the interference by recording information about the data subjects, the Court furthermore "scrutinise[s] the extent of the information which the police and security forces record".[1297] This scrutiny suggests that the proportionality assessment of the Court may have had a different outcome if other, or more information had been collected.

**ii. Personal Data Stored in Secret Police Files**

The case *Leander v. Sweden*[1298] of 1987 allowed the Court to refine its statements on necessity. *Leander* did not concern secret surveillance measures as such but rather the inclusion of a person in a secret register of security risks. Mr. Leander applied for a job as a carpenter in a museum attached to a naval base, but was not granted clearance to work in this museum due to an undisclosed security risk concerning his person.

While the Court began its assessment of the proportionality of the measure in question by stating that it can in general be deemed necessary "firstly, to collect

1295 ECtHR Case of *Murray v. the United Kingdom* [1994], paragraphs 92-93. See also Craig (1999), p. 88.
1296 McBride (1999), p. 27.
1297 Kilkelly (2003), p. 36.
1298 ECtHR Case of *Leander v. Sweden* [1987].

and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security."[1299] The Court then continued to examine the safeguards installed against a possible abuse of the system. The government of Sweden submitted a list of twelve safeguards, which cumulatively convinced the Court that the safeguards applicable to the measure were suitable to ensure that the measure in question met the requirements of Article 8 paragraph 2 of the ECHR.[1300] Particular attention was paid by the Court to "the fact that the supervision of the proper implementation of the system was entrusted both to Parliament and independent institutions",[1301] which went a long way to convince the Court that individuals were protected from arbitrariness and abuse of the system.

The notion of safeguards, so central in this case, requires some further explanation. The Article 29 Working Party explains this notion as follows:

> "The term safeguards in this context is also broad and may cover, for example, steps taken to limit the scope of a measure, or caveats placed upon when or how it can be exercised. Alternatively, it may involve requiring some other objective decision to be made prior to a measure being deployed in that case. Safeguards may also cover any rights of appeal afforded to individuals against a particular measure or its effects and the scope of those rights."[1302]

A different judgment of the ECtHR of 2006 connects neatly to this earlier case law. In *Segerstedt-Wiberg and Others v. Sweden*,[1303] the ECtHR was again confronted with a secret police register. The applicants in this case complained of the continued retention of records on them. One applicant, for instance, had visited a political meeting in Warsaw in 1967, data which, the Court found, may have been stored legitimately during the Cold War, but not thereafter.[1304]

1299 ECtHR Case of *Leander v. Sweden* [1987], paragraph 59.
1300 ECtHR Case of *Leander v. Sweden* [1987], paragraph 60 ff. See also Kilkelly (2003), p. 27, 36.
1301 Kilkelly (2003), p. 37.
1302 Article 29 Working Party, Opinion 1/2014, p. 10.
1303 ECtHR Case of *Segerstedt-Wiberg and Others v. Sweden* [2006].
1304 ECtHR Case of *Segerstedt-Wiberg and Others v. Sweden* [2006], paragraph 90.

The Court here did not base its assessment of the proportionality of the retention of these records on the availability of sufficient safeguards but rather on the reasons with which the government justified this continued retention, which is another parameter the Court uses to establish proportionality. In the case of the person attending a political meeting in Warsaw in 1967, the Court stated that "the Court, bearing in mind the nature and age of the information, does not find that its continued storage is supported by reasons which are relevant and sufficient as regards the protection of national security."[1305] Similarly, another applicant was entered into this register in 1969 with a note that he had advocated violent resistance to police control. The Court here also stated that the retention of this record "was supported by reasons that, although relevant, could not be deemed sufficient thirty years later."[1306] Based on the passing of time and the changed political climate in Europe, the Court found that the retention of these records "entailed a disproportionate interference with their right to respect for private life."[1307]

**iii. Taxation and Financial Data**

There is only meagre case law of the ECtHR on proportionality and financial data so far. The existing case law is made up by tax cases of rather similar histories. However, due to the role that financial data is playing in this dissertation, those cases should be highlighted briefly. One of the few relevant case is *X. v. Belgium*[1308] of 1982, a case which was dismissed by the Court as manifestly ill-founded and therefore only contains a very short and cursory examination.



In this case, the applicant was at a loss to explain what had become of the money he had received upon the sale of property. Beyond stating that part of the funds were invested in his own company, and part elsewhere, the applicant did not wish to disclose further details as to what had become of the funds, because "an obligation to give further details would compel him to reveal the most intimate aspects of private life."[1309] Therefore, the tax authorities made an estimate, but in

1305 ECtHR Case of *Segerstedt-Wiberg and Others v. Sweden* [2006], paragraph 90. See also Article 29 Working Party, Opinion 1/2014, p. 19; Korff (2014), p. 108.
1306 ECtHR Case of *Segerstedt-Wiberg and Others v. Sweden* [2006], paragraph 90.
1307 ECtHR Case of *Segerstedt-Wiberg and Others v. Sweden* [2006], paragraph 90.
1308 ECtHR Case of *X. v. Belgium* [1982].
1309 ECtHR Case of *X. v. Belgium* [1982], page 234.

calculating it, they also considered "a report established by an inspector referring to the applicants character and life style."[1310] The applicant challenged this estimate.

The Court, however, dismissed the case, stating that while there had been an interference, the measures taken by the tax authorities to learn the details of the applicant's investments were justified in the interest of the economic well-being of the state.[1311]

> "The principal problem to be decided in this case is whether and to what extent the exact collection of tax makes it necessary in a democratic society that the applicant, as a taxpayer, should disclose to the tax administration and, where necessary, present at a public hearing, the private use he has made of his assets.
>
> On the basis of the principles developed by the European Court in the above-mentioned Dudgeon case […], the Commission must determine whether the tax control measure complained of by the applicant is in proportion to the objective of the legislation, i.e. the public interest.
>
> The Commission therefore takes account of the fact that the cash sum which the applicant was unable or unwilling to prove that he had spent, was a considerable one and considers accordingly that it is not unreasonable for the tax authority to have required the applicant to provide details, although they concerned his private life, in order to establish that the capital in question was spent in a way that did not produce interest. The Commission notes that the applicant is not complaining about remarks made by a tax official on various aspects of his private and family life, remarks which played a role in the attitude adopted by the tax authorities towards him."[1312]

Based on those observations, the Court dismissed the case.

1310 ECtHR Case of *X. v. Belgium* [1982], page 234.
1311 See in this context also Beckmann (2017), p. 972.
1312 ECtHR Case of *X. v. Belgium* [1982], page 235 f. See also Feldman (1999), p. 127.

In the 1993 judgments in the cases *Miailhe v. France*,[1313] *Funke v. France*,[1314] and *Crémieux v. France*,[1315] the Court was again confronted with an interference with an individual's right to respect for private and family life in the interest of the collection of taxes.[1316] In these cases, the premises occupied by the applicants were searched by the authorities for the investigation of alleged tax crimes. While the Court in principle accepted that the measures were justified in the interest of the economic well-being of the state, it ruled that the measures in the form they were taking at the time were not necessary in a democratic society, due to the inadequate safeguards against abuse.[1317]

> "Undoubtedly, in the field under consideration - the prevention of capital outflows and tax evasion - States encounter serious difficulties owing to the scale and complexity of banking systems and financial channels and to the immense scope for international investment, made all the easier by the relative porousness of national borders. The Court therefore recognises that they may consider it necessary to have recourse to measures such as house searches and seizures in order to obtain physical evidence of exchange-control offences and, where appropriate, to prosecute those responsible. Nevertheless, the relevant legislation and practice must afford adequate and effective safeguards against abuse […].
>
> This was not so in the instant case. At the material time - and the Court does not have to express an opinion on the legislative reforms of 1986 and 1989, which were designed to afford better protection for individuals […] - the customs authorities had very wide powers; in particular, they had exclusive competence to assess the expediency, number, length and scale of inspections. Above all, in the absence of any requirement of a judicial warrant the restrictions and conditions provided for in law, which were emphasised by the Government […], appear too lax and full of loopholes for the interferences with the applicants' rights to have been strictly proportionate to the legitimate aim pursued."[1318]

1313 ECtHR Case of *Miailhe v. France* [1993].
1314 ECtHR Case of *Funke v. France* [1993].
1315 ECtHR Case of *Crémieux v. France* [1993].
1316 See, in this context, also Elias (1982), p. 207 ff.; Schweizer (2009), p. 464.
1317 McBride (1999), p. 27.
1318 ECtHR Case of *Miailhe v. France* [1993], paragraphs 37-38.

The Court therefore held that there was a violation of the applicants' rights under article 8 ECHR. In addition, this case is an interesting illustration as to the notion of adequate safeguards applied by the Court in cases concerning taxation.

A further case on taxation is the 2013 judgment in *Bernh Larson Holding v. Norway*.[1319] In this case, the financial records of a company were demanded and a backup copy was handed over for an audit. Problematic in this case was that the demands of the authorities were not supported by a judicial warrant, and that Bernh Larson Holding was using a mixed system with other companies, whose data was also affected by the investigation. The Court, however, accepted that even in the absence of a warrant, the condition of adequate safeguards was met.

> "It should also be observed that the nature of the interference complained of was not of the same seriousness and degree as is ordinarily the case of search and seizure carried out under criminal law, the type of measures considered by the Court in a number of previous cases […]. As pointed out by the Supreme Court, the consequences of a tax subject's refusal to cooperate were exclusively administrative […]. Moreover, the disputed measure had in part been made necessary by the applicant companies' own choice to opt for "mixed archives" on a shared server, making the task of separation of user areas and identification of documents more difficult for the tax authorities[…]."[1320]

This judgment suggests, therefore, that a judicial warrant is not the only possible way for a measure to meet the condition of adequate safeguards. Instead, the circumstances of each individual case must be reviewed carefully in order to assess the existing safeguards.

Not only is the existence of a warrant not entirely necessary, but the existence of a judicial warrant does not automatically mean that the existing safeguards can be considered to be adequate. This finding was made by the Court in the case *K.S. and M.S. v. Germany*.[1321] In this case, the competent authorities had purchased illegally obtained information on potential tax evaders. In these circumstances,

1319 ECtHR Case of *Bernh Larsen Holding AS and others v. Norway* [2013].
1320 ECtHR Case of *Bernh Larsen Holding AS and others v. Norway* [2013], paragraph 173.
1321 ECtHR, Case of *K.S. and M.S. v. Germany* [2016], paragraph 45.

the Court continues to make some interesting observations on the importance and proportionality of investigations into tax matters:

> "As to the proportionality of the search warrant to the legitimate aim pursued in the particular circumstances of the case, the Court, having regard to the relevant criteria established in its case-law, observes in the first place that the offence in respect of which the search warrant was issued was tax evasion, an offence which affects State' resources and their capacity to act in the collective interest. As such, tax evasion constitutes a serious offence; a fact underlined in a case such as this where the suspected tax evasion related to the sum of approximately EUR 100,000 (see, in this regard, the OECD Convention on Mutual Administrative Assistance in Tax Matters, developed in 1988 and amended in 2010, according to which the tackling of tax evasion forms a top priority for all member states). Furthermore, in this field - the prevention of capital outflows and tax evasion - States encounter serious difficulties owing to the scale and complexity of banking systems and financial channels and the immense scope for international investment, made all the easier by the relative porousness of national borders […]."[1322]

Therefore, taking into account not only the fact that the interest of the state in collecting taxes is directly related to its economic well-being and a policy priority in most countries,[1323] but also the fact that investigations into tax matters are necessarily very difficult, the Court considers the investigatory measures taken in this case to be proportionate to the legitimate aim pursued.



**iv. Personal Data and New Technologies**

The development of new technologies is also an important factor in the development of the principle of proportionality and the assessment of the proportionality of a given measure.[1324] A significant case in this regard is the case *S and Marper v. United Kingdom* of 2008.[1325] This case concerned a register kept by the authorities in the United Kingdom of DNA samples and fingerprints of

1322 ECtHR, Case of *K.S. and M.S. v. Germany* [2016], paragraph 48.
1323 See also Beckmann (2017), p. 972.
1324 See also Solove (2002), p. 1141 f.; Schertz (2013), p. 722; See for a discussion on new technologies, privacy, and proportionality Wright/Friedewald/Gellert (2015), p. 47 ff.
1325 ECtHR Case of *S. and Marper v. The United Kingdom* [2008].

criminal suspects.[1326] The applicants in this case have both not been convicted of a criminal offence, as the proceedings initiated against them had ended in an acquittal and a discontinuation, respectively.[1327] They therefore challenged the continued retention of their information in this database.

The Court begins its proportionality assessment with the general statement that "An interference will be considered necessary in a democratic society for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."[1328] It then continues to explain that "A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference."[1329] The margin of appreciation granted to the authorities is therefore narrower or wider depending on how much it interferes with the individual's rights. As the Article 29 Working Party notes,

> "This is important, as it means that 'necessity' should not be interpreted too broadly, as this would make it easier for fundamental rights to be circumvented. Nor should it be interpreted too literally, as this would set too high a bar and make it unduly difficult for otherwise legitimate activities which may justifiably interfere with fundamental rights to take place."[1330]

It should be noted that there is thus already a balancing act involved in the very interpretation of the term necessity as a criterion for proportionality.

A particularly important section of the judgment, concerning the applicability of new technology, follows. Both applicants had had their DNA samples and fingerprints taken in 2001, at a time in which the establishment of databases for

1326 See in this context also Santos (2012), p. 447.
1327 See also Maras (2012), p. 70; Galetta (2013), p. 9.
1328 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 101.
1329 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 102. See also the notes on the margin of appreciation in section (b) of this Chapter above.
1330 Article 29 Working Party, Opinion 1/2014, p. 6.

fingerprint and DNA material was still in its infancy in most states of Europe. England, Northern Ireland and Wales were among the forerunners of such databases, but were also the only jurisdiction among the contracting states of the ECHR who allowed for indefinite retention of such material, and failed to include any meaningful exceptions or safeguards.[1331] The government stated in its defence that while other states had provided for significant safeguards, those systems were much less advanced than its own and the approaches applied in different states could therefore not be compared with one another. This argument, however, was foreseeably rejected by the Court:

> "The Court cannot, however, disregard the fact that, notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life. The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."[1332]

This statement can be condensed into the principle that a pioneer in a technology must also be a pioneer in the proportionality assessment concerning that technology. In the following sections, the Court then assesses the proportionality of the challenged measures:

1331 It is notable that the applicant *S.* was arrested at the age of 11 and later acquitted of the charges raised against him. See also Article 29 Working Party, Opinion 1/2014, p. 19.
1332 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 112. See, in this context, also Leith (2006), p. 115.

> "In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the national database or the materials destroyed […]; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances."[1333]

Based on these defects, the Court could not but hold the measures to be disproportionate in relation to the aim pursued.

The Court had the opportunity to expand this line of case law also in *Szabó.*[1334] In this case the Court again stressed the obligation of states to use new technologies responsibly, in this case technologies that can be used for surveillance.

> "For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen […], especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development

1333 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 119. See also Feiler (2010), p. 16.
1334 ECtHR Case of *Szabó and Vissy v. Hungary* [2016].

> of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information[…]."[1335]

The concern of the ECtHR that overly broad surveillance measures taken in order to protect society from a certain threat, often terrorism and serious crime, may lead to the destruction of this democracy, has been emphasised already.[1336] The Court has expressed a very similar concern in the case *Roman Zakharov*, as quoted below.



An interesting case in the context of technology is also *Köpke v. Germany* of 2010.[1337] This case concerned a cashier in a supermarket, whose employer, suspecting her of theft, engaged a private investigator to collect evidence to this effect. The detective installed video surveillance of relevant areas of the supermarket, including of the cash register and Ms. Köpke working there, and collected decisive evidence based on which she was dismissed without notice. She challenged her dismissal before the labour courts, the German Constitutional Court, and finally the ECtHR.

1335 ECtHR Case of *Szabó and Vissy v. Hungary* [2016], paragraph 68.
1336 Böhme-Neßler (2016), p. 5 f. See in this context also Hadjimatheou (2014), p. 196.
1337 ECtHR Case of *Köpke v. Germany* [2010], Decision as to the Admissibility of the Application taken on 5 October 2010.

The ECtHR dismissed her application as manifestly ill-founded. The Court considered that the video surveillance was a reasonable step for the employer to take after having formed substantiated suspicions against Ms. Köpke, and that this step did not affect essential aspects of Ms. Köpke's private life.[1338] The Court then reviewed the proportionality assessment carried out by the labour courts, which balanced Ms. Köpke's right to privacy on the one hand against the rights and interests of her employer on the other hand, and came to the conclusion that the principle of proportionality was respected.[1339] The ECtHR found nothing to indicate that the lower courts had made a mistake, but it ended its review with an interesting statement. The ECtHR added,

> "The Court would observe, however, that the balance struck between the interests at issue by the domestic authorities does not appear to be the only possible way for them to comply with their obligations under the Convention. The competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies."[1340]

This statement is significant in that it very clearly states the need to reassess the proportionality of a measure when the technological circumstances change. This approach of the Court can be summed up by quoting a statement of the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism: "The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful".[1341]

An example of a successful proportionality assessment carried out by the national authorities and upon challenge accepted by the ECtHR was the subject of the case *Uzun v. Germany*.[1342] The case concerned GPS surveillance carried out against a suspect believed to be involved in a violent left-wing extremist group responsible

1338 ECtHR 420/07 *Köpke v. Germany* [2010], page 11.
1339 ECtHR 420/07 *Köpke v. Germany* [2010], page 12 f.
1340 ECtHR 420/07 *Köpke v. Germany* [2010], page 13.
1341 United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), p. 6.
1342 ECtHR Case of *Uzun v. Germany* [2010].

for several counts of attempted murder by bomb attacks. The measure in question was the tracking of the car of an accomplice of Uzun by means of a GPS device.[1343]

The Court found that Mr. Uzun's rights were not violated. In particular, the GPS device had only been attached to the car after less intrusive means of surveillance had failed. While the Court noted that the surveillance to which both Uzun himself and his accomplice had been subjected was extensive, it accepted that Mr. Uzun was only subjected to the GPS surveillance while travelling in his accomplice's car.[1344] A balancing of interests with the need to investigate the serious crime of attempted murder and the prevention of similar future offences on the one hand, and Mr. Uzun's right to privacy on the other hand led the Court to accept the proportionality of the measures taken against Mr. Uzun.[1345]

**v. Most Recent Case Law: Zakharov v. Russia**

One of the most recent cases the ECtHR has decided in this field is the case *Roman Zakharov v. Russia*.[1346] This case concerned an editor-in-chief of a publishing company, who challenged a measure according to which mobile phone operators were obliged to install equipment which enabled law enforcement authorities to intercept all telephone communications. The Court held that there was a violation of Article 8 of the ECHR.

In the first place, the challenged measure did not meet the minimum safeguards demanded of a measure of secret surveillance.

> "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the

1343 See also Murphy (2012), p. 457 ff.
1344 ECtHR Case of *Uzun v. Germany* [2010], paragraph 80.
1345 ECtHR Case of *Uzun v. Germany* [2010], paragraph 80. See in this context also Supreme Court of the United States, decision of January 23, 2012, *United States v. Jones*, 132 S.Ct. 945 (2012). This latter case is also discussed in Cate/Cate (2012), p. 264.
1346 ECtHR Case of *Roman Zakharov v. Russia* [2015].

> data to other parties; and the circumstances in which recordings may or must be erased or destroyed […]."[1347]
>
> "In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse."[1348]

In *Zakharov*, the Court also concerned itself with the question of suspicion and untargeted surveillance:

> "Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means […]."[1349]

This statement explicitly refers to the existence of suspicion in the context of surveillance, which can be read as an indication that indiscriminate mass surveillance is not sanctioned by the Court.[1350] However, this should only be considered an indication: a final answer to the question of mass surveillance has not yet been given by the ECtHR.[1351]

In summary, the law fails to adhere to the standard set by the ECtHR:

---

1347 ECtHR Case of *Roman Zakharov v. Russia* [2015], paragraph 231.
1348 ECtHR Case of *Roman Zakharov v. Russia* [2015], paragraph 232. See also Bülow (2013), p. 609; Galetta (2013), p. 10; Feiler (2010), p. 18; Ronellenfitsch (2007), p. 562.
1349 ECtHR Case of *Roman Zakharov v. Russia* [2015], paragraph 260. See also Tridimas (1999), p. 77.
1350 Article 29 Working Party, Working Document 1/2016, p. 8. See also Korff (2014), p. 108.
1351 Article 29 Working Party, Working Document 1/2016, p. 8.

> "The Court concludes that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications.[1352] In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. The domestic law permits automatic storage of clearly irrelevant data and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when 'necessary in a democratic society'. The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions."[1353]

An interesting point concerning the case *Roman Zakharov* is that the Court addressed the conditions "in accordance with the law" and "necessary in a democratic society" together. The Court stated that "'quality of law' in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when 'necessary in a democratic society', in particular by providing for adequate and effective safeguards and guarantees against abuse."[1354] It should be noted how the Court here emphasized the close relationship between those two points.



1352 See in this context also Huber (2007), p. 881 ff. Footnote added by the author.
1353 ECtHR Case of *Roman Zakharov v. Russia* [2015], paragraph 302. See also Boehm/De Hert (2012), p. 4; Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 342.
1354 ECtHR Case of *Roman Zakharov v. Russia* [2015], paragraph 236. See also Korff (2014), p. 89; Feiler (2010), p. 18.

**vi. Summary**

It is thus important to note that the ECtHR attaches a certain meaning to the formula "necessary in a democratic society", and that this meaning has changed and evolved over time, as well as depending on the circumstances of an individual case. To quote a criticism often made regarding the ECtHR's case law on the principle of proportionality, "The court has described its approach to striking such a balance in different ways in different contexts, and in practice often approaches the matter in a relatively broad-brush way."[1355] The case law of the ECtHR has described an arch from a rather guarded assessment of the proportionality of a measure in earlier case law to a more thorough assessment in later case law. The varied case law furthermore showed a flexible manner of addressing the question of proportionality, from which three distinct types of interpretation of the principle of proportionality can be distilled.

In the first place, in *Klass* and *Leander*, the Court applied the standard that "in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse".[1356] The existing safeguards for a measure were the main props on which the Court based its proportionality assessment in those early cases. The question of safeguards can, however, be linked to and seen as one element of a proportionality test demanding that measured not go beyond what is necessary. The proportionality test thus applied is a very broad test with endless possibilities for variation, depending on the context and the subject matter of an individual case.[1357] The question whether a measure goes beyond what is necessary is also seen as an effective safeguard against mass surveillance and other blanket measures, because there are almost always less intrusive means that can be employed.[1358] Further developments in this field are expected with interest.[1359]

1355 *Lord Reed* in Supreme Court of the United Kingdom, *Bank Mellat v Her Majesty's Treasury* (No. 2) [2013] UKSC 39 (19 June 2013), paragraph 70.

1356 ECtHR Case of *Leander v. Sweden* [1987], paragraph 60. See also Korff (2014), p. 108; De Hert (2003), p. 48. See also the fifth, tenth, eleventh, twelfth, and thirteenth concerns discussed in Chapter IX below.

1357 Article 29 Working Party, Opinion 1/2014, p. 10.

1358 Article 29 Working Party, Opinion 1/2014, p. 9. See also the parallels between ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 119 and CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 51 (discussed below). See also Feiler (2010), p. 16.

1359 ECtHR Case of *Big Brother Watch and Others v. the United Kingdom*, Application no.

A second but closely related line of case law was extended into the central question, whether the competent authorities could show 'relevant and sufficient reasons' for the introduction of interfering measures.[1360] This second test is often counted as a separate line taken by the ECtHR in its assessment of proportionality,[1361] but it is so closely connected to the concept of a 'pressing social need' that those can usually be viewed together.

In later case law, the pressing social need has moved more into the foreground of the assessment. The Court applied a more thorough test compared to its earlier cases, in which it did not just demand that the legislator's reasons were relevant and sufficient, but indeed that the legislator acted upon a 'pressing social need'. "An interference will be considered necessary in a democratic society for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'."[1362] While a conclusive definition of the term "a pressing social need" is still not developed, several notions can be distilled from the ECtHR's case law. Generally speaking, the notion of a pressing social need "will always involve identifying, within the broader sphere of the legitimate aim pursued, the specific societal need to be addressed with a view to protecting public security."[1363] In essence, the lawmaker is forced to define clearly the public interest it pursues with a given measure, and show how the interference with an individual's rights to privacy and data protection caused by this measure relates to public security. Not any public interest is suitable to be designated as 'pressing', however. This term "implies a greater level of severity, urgency or immediacy associated with the need that the measure is seeking to address."[1364] In effect, the condition of a 'pressing social need' must be evaluated on a case-by-case basis, using the Court's previous cases as guidance as to the legitimacy and urgency of the aim pursued by the lawmaker.

The different concepts of proportionality above identified are often applied individually but also often go together. A formula effectively covering the principle

58170/13, lodged on 4 September 2013, Communicated Case.

1360 See in this context also section (e) of Chapter IX below.

1361 Article 29 Working Party, Opinion 1/2014, p. 7.

1362 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 101.

1363 Article 29 Working Party, Opinion 1/2014, p. 7.

1364 Article 29 Working Party, Opinion 1/2014, p. 7. See also Barak (2013), p. 277 f.

of proportionality as applied by the ECtHR would therefore be the question whether certain measures go beyond what is necessary in order to address a pressing social need.

## d. Proportionality in European Union Law

Proportionality is a general principle of law under European Union law.[1365] There are a number of such general principles recognised in EU law, which take part in governing the policies of the European Union, particularly the law-making processes and the content of legislation.[1366] Among those principles are such very fundamental criteria as the rule of law,[1367] respect for human rights, non-discrimination, proportionality, subsidiarity, and the principle of conferral.[1368] Those general principles are of a constitutional value, which means that they are of such a high importance in the law-making procedure that a failure to respect them may give rise to an invalidation of a legal act.[1369]

The principle of proportionality is enshrined in Article 5 (4) of the Treaty on European Union. The principle of proportionality is one of the most important principles in law making, closely connected to the concept of rule of law.[1370] Basically, the principle means that any measure taken in order to achieve a certain legitimate aim must not go beyond what is necessary to achieve this aim. This means that among the potential measures that might be taken in order to achieve a certain legitimate aim, the legislator should choose the one measure which encroaches the least upon the rights and freedoms of the population.

### i. The Charter of Fundamental Rights of the European Union

After thus setting the principle of proportionality into its context, its relevance can be considered more closely. The principle of proportionality under European Union law comes into play on many different levels and in many different contexts,

1365 See also CJEU Case C-11/70, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* [1970]; Tridimas (1999), p. 69.
1366 Jacobs (1999), p. 1; Gerven (1999), p. 44 f.
1367 Barak (2013), p. 226 ff.
1368 Craig/De Búrca (2015), p. 550 ff.; European Commission (1999), p. 20 f. See also Benn (1984), p. 224 f.
1369 Hofmann in Barnard/Peers (2014), p. 203.
1370 Barak (2013), p. 232 f.

but the context most relevant for this thesis is that of human rights. According to the Charter of Fundamental Rights of the European Union, the fundamental rights enshrined within the Charter may only be limited under certain conditions. One of those conditions, and indeed the condition of the greatest relevance in practice, is that the principle of proportionality must be respected.

The Charter is the main human rights document in the European Union.[1371] Besides the human rights themselves, the principle of proportionality also plays a big role in the Charter of Fundamental Rights of the European Union. Article 52 (1) of the Charter, which defines the conditions under which rights and freedoms guaranteed in the Charter can be limited, states the following:

> "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

The principle of proportionality is therefore an express condition for the lawful limitation of any right enshrined in the Charter. Any legislative act to which the Charter is applicable must respect the rights and freedoms protected by the Charter. Therefore, whenever the limitation of a Charter right is challenged before the Court, the proportionality of the limitation must be examined closely.



**ii. Proportionality in the Law-making Procedure**

The principle of proportionality is not only applied by the Court upon a challenge, but must also be applied by the law-maker in the law-making procedure.[1372] Indeed, this principle is today a generally accepted component of the rule of law.[1373] It is found in numerous constitutions of states around the world and countless international treaties. As has already been mentioned, it is prominently enshrined in article 5 (4) of the Treaty on European Union, which reads, "Under the principle of proportionality, the content and form of Union action shall not exceed what

1371 See also Chapter V on privacy and data protection above.
1372 See also Feldman (1999), p. 124.
1373 Barak (2013), p. 226 ff.

is necessary to achieve the objectives of the Treaties." This provision is further fleshed out by Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality, attached to the Treaties by the Lisbon Treaty. According to Article 1 of that Protocol, "Each institution shall ensure constant respect for the principles of subsidiarity and proportionality, as laid down in Article 5 of the Treaty on European Union."

The institutions of the European Union must therefore comply with the principle of proportionality at all times. The most important instance in which this principle comes into play is, however, the law making procedure.[1374] Article 5 of the Protocol demands a clear statement justifying the proportionality of a legislative measures proposed in a draft legislative act. It goes on to state that "Any draft legislative act should contain a detailed statement making it possible to appraise compliance with the principles of subsidiarity and proportionality." The absence of such a detailed account can cause the CJEU to invalidate the legislative act in question, as will be seen in the discussion of the case law, particularly case *Schecke*, below.

Balancing of interests is, however, decidedly not an easy task. It is certainly not made easier by the fact that the Treaties, while demanding proportionality, are silent on the details of applying this principle. The details of the proportionality principle have been furnished by the CJEU in case law. The lawmaker must carefully examine the importance of all of the interests playing a role in a given measure, and weigh them against one another.

> "The basic balancing rule seeks to determine a legal rule that reflects all the elements of balancing between a law limiting a constitutional right and its effect on the constitutional right. It should reflect both ends of the scales as well as their relationship. It should apply in cases where both of the scales carry a constitutional right (such as a law limiting the freedom of expression in order to better protect the right to privacy), as well as in cases where the societal benefit scale carries public interest considerations (such as a law limiting the freedom of expression in order to better protect national security interests). Thus, such a balancing rule should reflect the marginal social importance of the benefits created by the limiting law (either to the individuals involved or to the public at large) as well as the marginal social importance in preventing the harm caused to the

1374 Gerven (1999), p. 58.

> limited right in question; it should also consider the probability of the occurrence of each. Such a basic balancing rule would be found within the constitutional limitation clause (either explicit or implicit)."[1375]

It almost goes without saying that this particular requirement is not always complied with properly. In the words of *Cicero*, "truly the most foolish thing is to think that everything is just that has been approved in the institutions or laws of peoples."[1376] This view of the proportionality assessment made by the law-maker is one of the reasons why the CJEU also reviews the proportionality of a given measure, with the potential outcome that that measure will be invalidated. For instance, in the currently ongoing legislative procedure concerning the fifth Anti-money laundering Directive,[1377] the Commission has been accused of falling short of the standards expected of a proportionality assessment concerning newly introduced measures.[1378] Indeed, it has been criticised that the task of looking after the rights to privacy and data protection is simply left to the Courts while the law-maker exclusively concerns themselves with the protection of (national) security and for the protection of that interest interferes with the fundamental rights of the population as far as it sees fit.[1379] The European Data Protection Supervisor laments that "the Commission seems to have foregone a proper proportionality assessment and have opted for 'blanket measures'."[1380] This accusation is based on the short and very general discussion of the measures introduced with the proposal. The following sections and Chapter IX below will go into details concerning aspects of this particular issue.



### iii. Margin of Appreciation and Judicial Restraint

In cases in which the proportionality of a measure contained in a legislative act of the European Union is disputed, the CJEU has exclusive jurisdiction to decide the matter. This possibility for a review of a legal act by the CJEU in order to test its compliance with the principle of proportionality, and the threat of invalidation

1375 Barak (2013), p. 363. *Barak* speaks of constitutional rights, but his rules eloquently sums up the process that must be followed also on the European level. See in this context also Raab (2014), p. 44.
1376 Cicero (2014), p. 42.
1377 See the proposal, COM (2016) 450 final.
1378 See for instance EDPS Opinion 1/2017, p. 12 ff.; Milaj/Kaiser (2017), p. 115 ff.
1379 Hornung/Schnabel (2009b), p. 119. *Hornung and Schnabel* criticize this situation for Germany, but the criticism is just as valid on the European level. See also Barak (2013), p. 487 f.
1380 EDPS Opinion 1/2017, p. 12. See also Feiler (2010), p. 16.

of an act found to be lacking in this regard, is the basis of the high importance assigned to this particular general principle.[1381] The numerous appeals to the CJEU to exercise this power has made the principle of proportionality the most frequently applied general principle in European Union law.[1382]

> "The Court has consistently held that the principle of proportionality is one of the general principles of Community law. By virtue of that principle, the lawfulness of the prohibition of an economic activity is subject to the condition that the prohibitory measures are appropriate and necessary in order to achieve the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued."[1383]

In practice, however, the Court generally limits itself to exercising a marginal review of whether or not the principle of proportionality was properly respected in the law-making procedure.[1384] The reason for such restraint is simply that the judicature must not sit on the chair of the lawmaker.[1385] In the Words of *Bradley*, "the legislature enjoys wide discretion, as it must make political, economic, and social choices on the basis of complex assessments; the Court will only intervene if the action taken is manifestly inappropriate to the objective sought by the measure."[1386] The choice of an instrument by which to address a public interest is therefore in principle left to the legislator. In the words of *Lord Reed and Lord Toulson*,

> "As a generalisation, proportionality as a ground of review of EU measures is concerned with the balancing of private interests adversely affected by such measures against the public interests which the measures are intended to promote. Proportionality functions in that context as a check on the exercise of public power of a kind traditionally found in public

1381 *Hofmann* in Barnard/Peers (2014), p. 203; Jacobs (1999), p. 5.
1382 *Hofmann* in Barnard/Peers (2014), p. 204.
1383 CJEU Case C-331/88 *The Queen v Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa and others* [1993], paragraph 13. See also Tridimas (1999), p. 70 f.
1384 *Bradley* in Barnard/Peers (2014), p. 116; Tridimas (1999), p. 70.
1385 Craig/De Búrca (2015), p. 577; Craig (1999), p. 85. See also Kant (1887), p. 165 f.
1386 *Bradley* in Barnard/Peers (2014), p. 116.

> law. The court's application of the principle in that context is influenced by the nature and limits of its legitimate function under the separation of powers established by the Treaties. In the nature of things, cases in which measures adopted by the EU legislator or administration in the public interest are held by the EU judicature to be disproportionate interferences with private interests are likely to be relatively infrequent."[1387]

The flexibility of the application of the principle of proportionality is also reflected in the margin of appreciation granted to the legislator. In principle, the Court operates under the assumption that the legislator is best able to judge how to regulate any aspect of law, and where the regulator is endowed with the power and freedom to make the decision as to how best to act, the Court interferes with this power and freedom as little as possible: "The broader the power of appraisal that the adopting institution has, the less comprehensive the review exercised by the Court."[1388]

An exception to this limited review is posed by the CJEU's review of the proportionality of measures involving a restriction to fundamental rights and freedoms, in which the CJEU applies the proportionality test more strictly than in other areas of law.[1389] The most recent case law in the field of privacy and data protection substantiates this trend. The line of case law in which the CJEU has invalidated a number of European Union acts on the basis of their disproportionate interference with the rights to privacy and data protection of the population will be discussed in detail below.



The discussion of the European concept of proportionality by the Supreme Court of the United Kingdom is also of particular interest because the concept of proportionality applied in the European Union is widely different than the standards applied in national law in the United Kingdom, which is incorporated in the *Wednesbury* principle.[1390]

---

1387 *Lord Reed and Lord Toulson* in United Kingdom Supreme Court, *Lumsdon & Ors, R (on the application of) v Legal Services Board* [2015] UKSC 41 (24 June 2015), paragraph 36. See also Feldman (1999), p. 124 f.
1388 Tridimas (1999), p. 76.
1389 Craig/De Búrca (2015), p. 577; Tridimas (1999), p. 76; Craig (1999), p. 102.
1390 De Búrca (1997), p. 573.

> "The case law is full of judicial reminders of the sovereignty of Parliament and the related accountability of administrative bodies, and emphatic assertions of the difference between review and appellate jurisdiction. The *Wednesbury* principle, as is well known, holds that a discretionary decision of a public authority should be quashed by the courts only if it is 'so unreasonable that no reasonable authority could ever come to it', whereas the principle of proportionality, as it has been developed in EC and ECHR case law, holds that the decision of a public body should be quashed if its adverse effects on a legally protected interest or right go further than can be justified in order to achieve the legitimate aim of the decision."[1391]

This example serves well to illustrate the struggle some national legal systems have had in order to accommodate the European principle of proportionality. The national concepts of proportionality, necessity, and balancing of rights and interests as well as of judicial review of legislation are often clashing with the European notion of proportionality. This way, the German concept of proportionality is developed in more depth and detail,[1392] and the French legal system applies a system of proportionality which is equally as vague as the European principle of proportionality.[1393] Surely the marked differences in national law are also a factor that led to the heterogeneity of the European approach.

**iv. The Proportionality Test as Applied by the CJEU**

In order to review the proportionality of a legislative measure, the CJEU applies a test. The proportionality test as now applied by the CJEU consists of three steps. These three steps are the appropriateness or suitability of the measures to achieve a certain aim, the necessity of the measure in order to achieve the objective, and the proportionality in *stricto sensu*, in which the Court assesses the fairness of the balance struck between the limitations of fundamental rights on the one hand, and on the other hand the importance of the achievement of the objective at which the measure aims.[1394] It should be pointed out that the proportionality test

1391 De Búrca (1997), p. 562.
1392 Gerven (1999), p. 44 f.; Barak (2013), p. 178 f.
1393 Gerven (1999), p. 48 f.
1394 Barak (2013), p. 340 ff.

is by no means applied consistently.[1395] The circumstances of each individual case determine how the Court applies its criteria, with significant possibilities to vary the assessment if necessary.[1396] In particular the boundaries between the second and third step are often blurred and they may be considered together.[1397] However, the Court does carry out its three-step assessment whenever it deems it advisable to do so, and usually all of the Court's observations fit into the three criteria so outlined. Therefore, the three-step assessment will be presupposed throughout this thesis.[1398]

Before going into further detail, it is important to discuss the requirements for a legitimate aim. The legitimacy of the public interest objective pursued by a measure is a precondition for the proportionality test.[1399] An objective which is not in the public interest cannot justify the infringement of protected rights and freedoms, and therefore the proportionality of measures taken in order to achieve such an objective needs not be tested, as they will be invalidated on those grounds already.[1400] Naturally, however, the range of legitimate interests is extremely broad: All sorts of economic, political, or social aims may be legitimate objectives in the public interest.[1401] As will be discussed in section (f) of the following Chapter IX, the fight against serious crime, particularly against money laundering and terrorist financing, is also generally considered to be a legitimate objective in the public interest.

In the presence of a legitimate aim, the proportionality test can be applied. The first step of the proportionality test is the question, whether the measure concerned is an appropriate measure at all, i.e. whether the measure is suitable to achieve the objective pursued with this measure. This element of the proportionality test is most often of relevance when the CJEU tests measures taken by Member States, which infringe upon the fundamental freedoms in order to achieve a certain objective in the general public interest.[1402] In other areas, such as in the field of



1395 Jacobs (1999), p. 2; Tridimas (1999), p. 68.
1396 Gerven (1999), p. 39.
1397 Tridimas (1999), p. 68.
1398 In particular, this three step assessment will be applied in Chapter IX below in order to assess the proportionality of the anti-money laundering measures.
1399 Tridimas (1999), p. 66.
1400 Barak (2013), p. 251.
1401 Trstenjak/Beysen (2012), p. 273; Barak (2013), p. 252.
1402 Trstenjak/Beysen (2012), p. 271. See also Gerven (1999), p. 39; Tridimas (1999), p. 68.

human rights, this element is of a lower importance compared to the other two elements.

The second step of the proportionality test is the question, whether the measure concerned goes beyond what is necessary in order to achieve the aim in question.[1403] This second component of the proportionality test is more often the crucial element of the test. The purpose of this step is to make sure that fundamental rights and freedoms guaranteed by European Union law are always only limited to the extent which is absolutely necessary in order to achieve the aim pursued by the measure in question.[1404] It should be pointed out that necessity and usefulness are decidedly not the same thing. As the Article 29 Working Party points out in this context, the legislator must prevent be sure that any newly proposed measures are not simply considered of '"added value' or 'being useful"'.[1405] Anything going beyond what is necessary in order to achieve the aim is not per se necessary and therefore in principle disproportionate.[1406]

The final step of the proportionality test is the question, whether a measure is proportionate in *stricto sensu*, i.e. whether the steps taken are reasonable.[1407] The reasonableness of a measure can be accepted if the costs in the shape of a limitation of a fundamental right or freedom are fairly balanced with the benefits in the shape of the achievement of an objective in the public interest.[1408] Assessing the fairness of such a balance is exceedingly difficult and a matter in which the CJEU generally limits itself to a very marginal review.[1409] The assessment of this balance would depend on the value assigned to both the fundamental right or freedom on the one side, and the public interest objective on the other hand. Those values are defined differently by different persons and are prone to change over time.[1410] In

1403 Barak (2013), p. 317 ff.
1404 See also Rawls (2001), p. 104.
1405 Article 29 Working Party, Opinion 1/2014, p. 3. See also similarly ECtHR Case of *Handyside v. the United Kingdom* [1976], paragraph 48.
1406 Trstenjak/Beysen (2012), p. 271 f.; Article 29 Working Party, Opinion 1/2014, p. 3.
1407 Barak (2013), p. 340 ff. See in this context also Craig (1999), p. 88.
1408 Gerven (1999), p. 45; Leith (2006), p. 112.
1409 Trstenjak/Beysen (2012), p. 273 f.; Gerven (1999), p. 38 f.
1410 The concept of non-discrimination is a good example: the value of the principle of non-discrimination on the grounds of, among others, in particular gender and sexual orientation has undergone an immense and rapid change, with discrimination being practically the norm in the 1950's and 1960's, during the early years of the European Union. See also the discussion of the impact of new technology on the proportionality review of the ECtHR above. See also Article 29 Working Party, Opinion 1/2014, p. 7 f.

its assessment, the Court therefore only places the different interests involved in the dispute into relation to one another, and assesses whether the balance struck by the lawmaker remains within the boundaries of reason.[1411]

**v. Suitability of a Measure**

As has already been outlined above, the first step in the proportionality assessment of a given measure is the examination of the question, whether the measures are suitable to achieve the stated aim. In practice, however, this question is of relatively minor importance. Indeed, the CJEU largely limits itself to examining whether the measures in question are not evidently unsuitable to reach a certain aim. The Court has frequently emphasised that "the criterion to be applied is not whether the measure adopted by the legislature was the only one or the best one possible but whether it was manifestly inappropriate."[1412]

> "As a preliminary point, it ought to be borne in mind that the principle of proportionality, which is one of the general principles of Community law, requires that measures implemented through Community provisions should be appropriate for attaining the objective pursued and must not go beyond what is necessary to achieve it […].
>
> With regard to judicial review of the conditions referred to in the previous paragraph, the Community legislature must be allowed a broad discretion in an area such as that involved in the present case, which entails political, economic and social choices on its part, and in which it is called upon to undertake complex assessments. Consequently, the legality of a measure adopted in that sphere can be affected only if the measure is manifestly inappropriate having regard to the objective which the competent institution is seeking to pursue […]."[1413]



1411 Trstenjak/Beysen (2012), p. 273.

1412 CJEU Case C-189/01, *H. Jippes, Afdeling Groningen van de Nederlandse Vereniging tot Bescherming van Dieren and Afdeling Assen en omstreken van de Nederlandse Vereniging tot Bescherming van Dieren v Minister van Landbouw, Natuurbeheer en Visserij* [2001], paragraph 83. See also Craig (1999), p. 85.

1413 CJEU Case C-491/01, *The Queen v Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd* [2002], paragraphs 122-123. See also Tridimas (1999), p. 71.

However, these explanations of the Court only provide limited clarity, as the notion of manifest inappropriateness has not yet been further defined by the Court. The absence of a definition of the term 'manifestly inappropriate' has therefore given rise to some speculation as to the threshold of unsuitability that the Court would require for invalidation of a measure:

> "The court has not explained how it determines whether the inappropriateness of a measure is or is not manifest. Its practice in some cases suggests that it is sufficient to establish that there is a clear and material error, in law, or in reasoning, or in the assessment of the facts, which goes to the heart of the measure. In other cases, the word "manifestly" appears to describe the degree of obviousness with which the impugned measure fails the proportionality test. In such cases, the adverb serves, like comparable expressions in our domestic law, to emphasise that the court will only interfere when it considers that the primary decision-maker has exceeded the generous ambit within which a choice of measures might reasonably have been made."[1414]

Not surprisingly, the CJEU has invalidated only few measures on the grounds that they were unsuitable to achieve a legitimate aim in the past. The elements of necessity and proportionality in *stricto sensu* are of greater practical importance in most of the CJEU's case law on restrictions to fundamental rights.[1415]

## e. Necessity and Proportionality in the Case Law of the CJEU

The case law of the CJEU on the proportionality of interferences with the rights to privacy and data protection is going to be the basis for the assessment of the proportionality of the measures of the Anti-money laundering Directive in Chapter IX below. The case law of the CJEU is particularly authoritative, as it is in principle exclusively competent to assess the legality of a European Directive.

1414 *Lord Reed and Lord Toulson* in United Kingdom Supreme Court, *Lumsdon & Ors, R (on the application of) v Legal Services Board* [2015] UKSC 41 (24 June 2015), paragraph 42. See also Craig (1999), p. 88.
1415 Tridimas (1999), p. 71. See also Barak (2013), p. 317 ff.

Therefore, the case law of the CJEU in this field will be discussed in the present section.

**i. Interferences with the Rights to Privacy and Data Protection**

To examine the elements of necessity and proportionality in *stricto sensu*, the case law of the Court must be examined. The principle of proportionality has frequently been applied by the CJEU in its case law. In fact, the principle of proportionality lies at the core of the majority of case law of the CJEU concerning restrictions to rights contained in the Charter and the four fundamental freedoms. However, the great amount of case law still did not solve all questions of proportionality, but only created limited certainty in specific cases.

In principle, the Court always applies the same test, but there are nuances to this test, depending on a large number of variables. Proportionality is always assessed with regard to specific interests which must be balanced, and with regard to the actors involved. Therefore, the proportionality assessment of the CJEU in cases of restrictions to fundamental freedoms by Member States are very different from assessments in cases concerning interferences with human rights by measures contained in a directive.[1416] The different natures of the concepts of fundamental rights and freedoms make it difficult to apply findings of the Court in the context of fundamental freedoms to cases of fundamental rights.[1417] Equally, the great variety of fundamental rights make it difficult to draw comparisons between cases concerning the rights to privacy and data protection to, say, the right to property or a fair trial.



Therefore, in this section, only cases concerning the proportionality of interferences with the rights to privacy and data protection are considered. Due to the importance of, firstly, the context and the facts of the case for the proportionality review in case law, as well as, secondly, the development of the principle of proportionality over time, the cases selected for discussion have been structured roughly by subject matter and in chronological order.

1416 Craig/De Búrca (2015), p. 551 ff. See also Gerven (1999), p. 51; Barak (2013), p. 488 f.
1417 *Hofmann* in Barnard/Peers (2014), p. 204. On the application of the principle of proportionality specifically to data protection, see Tranberg (2011), p. 240 ff.

### ii. Early Cases: Rechnungshof and Lindqvist

As the Charter of Fundamental Rights is a relatively new human rights document, being only of the year 2000, the earliest data protection and privacy case law of the CJEU still refers to Article 8 of the ECHR as a standard. One of the cases in which the CJEU refers to both the ECHR as well as to case law of the ECtHR is the case *Rechnungshof* of 2003.[1418] This case concerned Austrian legislation which required the publication of income data of persons employed by the state in various capacities. The purpose of this publication of income data was increased transparency: the public availability of income data was intended to ensure that the salaries of civil servants are kept within a reasonable limit. However, the publication of the names of each employee was challenged before the Court.

In its discussion of the question of proportionality, the Court uses the formula employed by the ECHR: "It must be ascertained whether the interference in question is necessary in a democratic society to achieve the legitimate aim pursued."[1419] The Court begins by accepting the legitimacy of the interest of the state in ensuring the economical use of public funds, and concedes the suitability of the measures taken.[1420] However, the crux of the matter lies in the question, whether or not the publication of the names of the employees went beyond what is necessary in order to achieve this aim. The important question is, therefore, whether the measures were "proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient."[1421]

In the end, the Court left the decision over the proportionality of the publication of the names of the civil servants up to the national courts, but with some words of guidance. While accepting the legitimate interests of the state on the one hand, the Court states that

1418 CJEU Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof* (C-465/00) v Österreichischer Rundfunk and Others, *and Christa Neukomm* (C-138/01) and *Joseph Lauermann* (C-139/01) v Österreichischer Rundfunk [2003]. See also Lynskey (2014), p. 575.

1419 CJEU Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003], paragraph 82.

1420 CJEU Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003], paragraphs 84 f.

1421 CJEU Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003], paragraph 86. See also EDPS Opinion 1/2017, p. 14.

> "It is for the national courts to ascertain whether such publicity is both necessary and proportionate to the aim of keeping salaries within reasonable limits, and in particular to examine whether such an objective could not have been attained equally effectively by transmitting the information as to names to the monitoring bodies alone. Similarly, the question arises whether it would not have been sufficient to inform the general public only of the remuneration and other financial benefits to which persons employed by the public bodies concerned have a contractual or statutory right, but not of the sums which each of them actually received during the year in question, which may depend to a varying extent on their personal and family situation.
>
> With respect, on the other hand, to the seriousness of the interference with the right of the persons concerned to respect for their private life, it is not impossible that they may suffer harm as a result of the negative effects of the publicity attached to their income from employment, in particular on their prospects of being given employment by other undertakings, whether in Austria or elsewhere, which are not subject to control by the Rechnungshof."[1422]

In the same year in which the Court decided in the *Rechnungshof* case, it also decided *Lindqvist*.[1423] This case concerns the disclosure of personal data over the internet by a private individual, and although proportionality plays a minor role in the judgment, the Court does add an important detail in its assessment. In the decision, it is stated that



> "In that context, fundamental rights have a particular importance, as demonstrated by the case in the main proceedings, in which, in essence, Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site.

1422 CJEU Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* [2003], paragraphs 88-89.
1423 CJEU Case C-101/01, *Criminal proceedings against Bodil Lindqvist* [2003].

> Consequently, it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality."[1424]

Therefore, the main take-away from this early case law of the CJEU is that while the Court accepts that the national lawmaker enjoys a wide margin of appreciation, that discretion finds its limits in the proportionality principle. This is the basis for the application of the principle of proportionality and the reason for its great importance in practice.[1425]

### iii. The Right to Privacy and the Interests of Copyright Holders

The right to privacy and data protection was challenged particularly often by representatives of holders of copyright. Digital processing and transfer of data makes it easy to infringe upon copyright, and frequently right holders demand the identification of alleged infringers by internet service providers granting access to the internet to those persons. The internet user's rights to privacy and data protection therefore collide with the interest of the right holders in adequately protecting their rights.

One of the first cases of this nature is the 2008 decision in *Promusicae*.[1426] Promusicae was a representative of right holders who wished to bring civil action against persons using a popular file sharing service. It demanded that internet service providers identified certain users accessing that file sharing service, which the provider refused to do. The task of the CJEU was therefore to offer guidance on the reconciliation of conflicting fundamental rights, being the rights to privacy and data protection (articles 7 and 8 of the Charter) on the one hand, and the right to the protection of intellectual property and to an effective remedy (articles 17 and 47 of the Charter) on the other hand.[1427] In its decision, the CJEU repeated and elaborated upon its guidance on proportionality already stated in *Lindqvist*.

1424 CJEU Case C-101/01 *Lindqvist* [2003], paragraph 86-87.
1425 Tranberg (2011), p. 240 f.
1426 CJEU Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008]. See also Michl (2017), p. 351.
1427 CJEU Case C-275/06 *Promusicae* [2008], paragraphs 65 f. See also Lynskey (2014), p. 576.

The Court emphasised that "Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order."[1428]

A later case of with a very similar background is *SABAM*, decided by the CJEU in 2011.[1429] The question in this case went further than that in *Promusicae*, however, as in this later case a system of active monitoring of the connections of internet users was suggested, in order to effectively prevent infringement of copyright. The CJEU rejected the introduction of such a system on the basis of disproportionate interference with the right of internet service providers to conduct a business.[1430] The Court continued to examine the proportionality of such as system in relation to the right of the internet user and came to the conclusion that the principle of proportionality would not be respected in this context either.[1431] As it had already established a disproportionality in another context, however, the CJEU kept its observations on the privacy of users very general.

A third case concerning the balancing of the rights to privacy and data protection with the rights of copyright holders is *Bonnier Audio*.[1432] The facts of this case are again very similar to those of *Promusicae*, and the CJEU therefore kept its assessment of the proportionality short. It did add a short note on the proportionality of the applicable law which is of interest. The national law governing the disclosure of the identity of an internet user required clear evidence of an infringement and a proportionality assessment in each individual case.[1433] The CJEU thus ruled that "such legislation must be regarded as likely, in principle, to ensure a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the protection of personal data enjoyed by internet subscribers or users."[1434]

The Court therefore consistently demands that the lawmaker leaves sufficient room in its national law for the balancing of fundamental rights against one another.[1435]

1428 CJEU Case C-275/06 *Promusicae* [2008], paragraphs 70.
1429 CJEU Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011].
1430 CJEU Case C-70/10 *SABAM* [2011], paragraph 49. See also the seventh concern discussed in Chapter IX below.
1431 CJEU Case C-70/10 *SABAM* [2011], paragraphs 50 f.
1432 CJEU Case C-461/10, *Bonnier Audio AB and Others v Perfect Communication Sweden AB* [2012].
1433 CJEU Case C-461/10 *Bonnier Audio* [2012], paragraph 58 f.
1434 CJEU Case C-461/10 *Bonnier Audio* [2012], paragraph 60.
1435 CJEU Case C-275/06 *Promusicae* [2008], paragraphs 70.

As could be distilled particularly from the case *Bonnier Audio*, a system which demands a balancing of the interests involved on both sides in each individual case before disclosing a data subject's identity is the best option to ensure consistent respect for the principle of proportionality.[1436] This way the Court ensures sufficient room for a case-by-case assessment as far as possible.

**iv. Information on the Balancing of Interests**

Two cases should be highlighted in which the Court expanded upon the importance of the proper explanation of the interests involved in the balancing of interests. The first of those cases concerns the information to be supplied to an interested party,[1437] and the second case concerns the documentation of the balancing by the lawmaker.

The case *Bavarian Lager*[1438] concerned a request for information of a trade association to access unredacted minutes of a meeting organized by the Commission. The Commission had disclosed the minutes of the meeting but had removed the names of some of the persons present at that meeting because it could not obtain the consent of those persons for the disclosure of their data. The Commission had rejected Bavarian Lager's request for the names of those persons on the basis that Bavarian Lager could not establish why it was necessary that it should learn the identities of the attendees.[1439]

The Court confirmed the Commission's assessment, stating that

> "As Bavarian Lager has not provided any express and legitimate justification or any convincing argument in order to demonstrate the necessity for those personal data to be transferred, the Commission has not been able to weigh up the various interests of the parties concerned. Nor was it able to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced".[1440]

1436 CJEU Case C-461/10 *Bonnier Audio* [2012], paragraph 60.
1437 See on the conflict between privacy and the public access to documents Docksey (2016), p. 195 ff.
1438 CJEU Case C-28/08 P, *European Commission v The Bavarian Lager Co. Ltd* [2010].
1439 CJEU Case C-28/08 P *Bavarian Lager* [2010], paragraph 77. See also Lynskey (2014), p. 577.
1440 CJEU Case C-28/08 P *Bavarian Lager* [2010], paragraph 78. Lynskey (2014), p. 579 argues that according to this judgment, the "data protection rules must systematically prevail over EU rules on freedom of information", which is a view that is not compatible with a consistent application of the principle of proportionality.

The responsibility to establish a legitimate interest therefore clearly lies with the applicant in such cases.[1441]

Not only is an interested party obliged to document its legitimate interest when requesting data, but the authority's act of balancing this interest against other interests involved must also be documented.[1442] This latter obligation comes into play in the law-making procedure. The documentation of the balancing act was a problem in case *Schecke*,[1443] in which the CJEU criticised the lack of evidence of a balancing of interests having taken place in a law-making procedure. The measure in question was the obligation to disclose the recipients and amounts of subsidies received from agricultural funds. The applicants challenged this measure on the grounds of the interference of such disclosure with their rights to data protection and privacy.

The Court criticised the irreproducibility of the balancing of interests.[1444]

> "As far as natural persons […] are concerned, however, it does not appear that the Council and the Commission sought to strike such a balance between the European Union's interest in guaranteeing the transparency of its acts and ensuring the best use of public funds, on the one hand, and the fundamental rights enshrined in Articles 7 and 8 of the Charter, on the other."[1445]



Such a balancing ought to have taken place, regardless of the value the Commission placed on the interest in transparency. The Court went on to state very clearly that "No automatic priority can be conferred on the objective of transparency over the right to protection of personal data […], even if important economic interests are at stake."[1446]

1441 Case C-28/08 P *Bavarian Lager* [2010], paragraph 78 f.; Barak (2013), p. 252 ff.
1442 See in this context also Hansen (2016), p. 588 f.
1443 CJEU Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR* (C-92/09) *and Hartmut Eifert* (C-93/09) *v Land Hessen* [2010]. See also Michl (2017), p. 351.
1444 Skouris (2016), p. 1360. See also Article 29 Working Party Opinion 14/2011, p. 11 on the importance of the clear documentation of a data protection assessment before the adoption of legislation.
1445 CJEU Joined cases C-92/09 and C-93/09 *Schecke* [2010], paragraph 80.
1446 CJEU Joined cases C-92/09 and C-93/09 *Schecke* [2010], paragraph 85. See also Posner (1984), p. 344 f.

The CJEU's judgment in *Schecke* can be read as a positive obligation on the side of the lawmaker to document that a balancing of interests has taken place in the law-making procedure.[1447] If such a balancing act cannot be shown, and "it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the European Union rules in question,"[1448] the lawmaker had not shown the due respect to the principle of proportionality and the legislation in question had to be invalidated.[1449]

This line of case law is of immense relevance, as it forces the lawmaker to justify not only the measures it takes as serving a legitimate interest, but to go into details of the design of the measures chosen and the proportionality of this design. It allows better insights into the lawmaker's view of whether the measures in question go beyond what is necessary to achieve their aim. Since this question is often the most important question in the proportionality assessment of a given measure, the lawmaker's statements about this question are of great importance in practice.[1450]

### v. Strengthened Protection of the Right to Privacy: Digital Rights Ireland and Tele2 Sverige

In the most recent case law of the CJEU, there were several high profile privacy and data protection cases, beginning with *Digital Rights Ireland* and *Google Spain* in 2014, *Schrems* in 2015, and most recent *Tele2 Sverige* in 2016. All those cases are characterised by an emphasis on the proportionality principle, and the great value the CJEU awarded to the rights to privacy and data protection.[1451]

*Digital Rights Ireland*[1452] is the first case in this series of high-profile cases and the most influential one, the terms of which are invoked by the Court in all subsequent judgments. In this case, the CJEU has found very clear words to

1447 Tranberg (2011), p. 245 f.
1448 CJEUJoined cases C-92/09 and C-93/09 *Schecke* [2010], paragraph 86. See also Streinz (2011), p. 605.
1449 CJEU Joined cases C-92/09 and C-93/09 *Schecke* [2010], paragraph 89; Skouris (2016), p. 1360.
1450 In this way, the Commission's discussion of the proposals of the fourth and fifth Anti-money laundering Directives are two of the most important sources for the assessment of the proportionality of the anti-money laundering measures, conducted in Chapter IX below.
1451 Skouris (2016), p. 1362; Fuster (2016), 184 f. See also Goemans/Dumortier (2003), p. 162 f.
1452 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (C-293/12) *v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung* (C-594/12) *and Others* [2014].

describe the disproportionality of the data retention measures challenged before it. It is therefore also widely considered one of the most important human rights decisions of the CJEU in the past decade.[1453] This case was the first of the line of the CJEU's ground-breaking data protection and privacy decisions of recent years.

Subject of a series of high-profile litigation was the Data retention Directive 2006/24/EC,[1454] which demanded the retention of all connection and traffic data registered by service providers of communication services for a period of six to 24 months in order to allow law enforcement authorities access to this data in the fight against serious crime.[1455] In its decision in *Digital Rights Ireland*, the Court decided that the measures contained in the EU Data retention Directive went beyond what is necessary to achieve the aim pursued by these measures, namely the fight against serious crime. The Court found words of an unprecedented fierceness and clarity to describe the failure of the lawmaker to respect the principle of proportionality.[1456] This judgment will be of great importance to the following Chapter IX, where *Digital Rights Ireland* and *Tele2 Sverige* will serve as the main foothold for the proportionality assessment of the Anti-money laundering Directive. The discussion of the CJEU's assessment of the proportionality of the Data retention Directive will therefore be explained in some detail.[1457]

The Court begins its assessment by stating

> "As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not,



1453 Skouris (2016), p. 1364.
1454 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63 [no longer in force].
1455 Goemans/Dumortier (2003), p. 162 f.
1456 Skouris (2016), p. 1361; Koshan (2016), p. 168; Danwitz (2015), p. 582.
1457 See also section (b) of Chapter IX below.

> in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight."[1458]

The Court then continued to criticise the seriousness of the interference, based on, in the first place, the lack of personal exceptions to the retention scheme. The Directive simply covered in a very general manner all users of telecommunications services, which, as the Court correctly pointed out, is the great majority of the members of the society.

> "Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.
>
> Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."[1459]

In addition, the Court emphasised the lack of procedural safeguards contained in the Data retention Directive.

---

1458 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 51. See also Skouris (2016), p. 1364; Tridimas (1999), p. 77; Solove (2007), p. 411; Waldron (2003), p. 191 f.
1459 CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraphs 58-59. See also Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 337 f.; Danwitz (2015), p. 582.

> "Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.
>
> Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements."[1460]



Finally, in addition to the lack of personal exceptions, the Directive moreover lacked any meaningful material exceptions. It did not specify particular sets of data which were to be retained, or specified sets of data which could be deleted earlier. Instead, it simply introduced a blanket retention measure applicable to all data.[1461]

> "Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible

1460 CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraphs 60-61. See also Milaj/Kaiser (2017), p. 121. Danwitz (2015), p. 582.
1461 Feiler (2010), p. 16.

> usefulness for the purposes of the objective pursued or according to the persons concerned.
>
> Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary."[1462]

Based on those main arguments, the Court held that the lack of exceptions and safeguards in the Directive was incompatible with the principle of proportionality. It summarily invalidated the Directive.[1463]

In the second case concerning measures of data retention, *Tele2 Sverige*,[1464] the Court repeated its findings in *Digital Rights Ireland* in its assessment of the proportionality of national data retention regimes. This case, decided two years after *Digital Rights Ireland*, concerned the national laws originally adopted to implement the by the invalidated Directive.[1465] In this case, the CJEU repeated its proportionality assessment of *Digital Rights Ireland* with one significant addition. In *Tele2 Sverige*, the Court formulates positive criteria which a law must fulfil in order to be considered proportionate.

In its decision in *Tele2 Sverige*, the Court stressed the need for appropriate safeguards in the national data retention legislation. "A data retention measure must […] lay down clear and precise rules" according to which access to the retained data can be granted to the competent authorities, which "must be legally binding under domestic law."[1466] The Court continued to stress that clear and precise rules really rule out the use of broad general clauses.

> "In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national

1462 CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraphs 63-64.
1463 See also Article 29 Working Party, Opinion 1/2014, p. 12.
1464 CJEU Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016].
1465 Danwitz (2015), p. 583.
1466 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 117. See also Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 338.

> law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data […]."[1467]

Finally, the Court demanded that access should, if possible, be granted only in the presence of a warrant for this access, that the data subject must be notified of data being accessed, that data security must be ensured.[1468]

> "Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime […]. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.
>
> In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established



1467 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 118. See also Milaj/Kaiser (2017), p. 121.
1468 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 120 ff. See also Hamacher (2006), p. 636 f.; Korff (2014), p. 104 f.; Herrmann/Soiné (2011), p. 2924 f.; Gurlit (2010), p. 1039.

> urgency,[1469] be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime […]."[1470]

Based on its considerations, the CJEU ruled that legislation such as the data retention rules at issue in this case, was incompatible with articles 7 and 8 in connection with article 52 (1) of the Charter.

These two cases are notable for their in-depth analysis of the proportionality of measures limiting the rights to privacy and data protection of the population. Particularly *Tele2 Sverige* goes beyond the previous case law by defining clear minimum standards which national legislation must comply with in order to satisfy the conditions set out in the Charter. Chapter IX is devoted entirely to a further discussion of the findings of the CJEU in those two cases, by applying these findings of the Court to the Anti-money laundering Directive.

**vi. Privacy and Individual Interests: Google Spain**

Closely on the heels of the CJEU's decision in *Digital Rights Ireland*, the Court decided the case *Google Spain*.[1471] This case concerned the demand of a private individual that certain newspaper articles concerning him no longer appeared in the search results appearing in response to a search for his name. Therefore, the rights of the individual to privacy and data protection had to be balanced against the economic interests of the service provider.[1472] Concerning this question, the CJEU very clearly stated that a serious interference with the rights to privacy and data protection "cannot be justified by merely the economic interest which the operator of such an engine has in that processing."[1473]

---

1469 See in this context also Barak (2013), p. 277 f. Footnote added by the author.
1470 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraphs 119-120. See also Feldman (1999), p. 134.
1471 CJEU Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014]. See also the analysis of the case in Van Alsenoy/Koekkoek (2015), p. 105 ff.
1472 Caspar (2015), p. 589 f.; Leutheusser-Schnarrenberger (2015), p. 587 f.
1473 CJEU Case C-131/12 *Google Spain* [2014], paragraph 81. See also Skouris (2016), p. 1361; Posner (1984), p. 344 f.

In addition, the rights of the data subject had to be balanced against the right to information of other members of the public. Concerning this balancing act, the approach of the Court is more nuanced. In the beginning, the Court stated with clarity that in principle, the rights of the data subjects outweigh the interests of the internet user in gaining access to information.[1474] However, the balance of interests does depend on the circumstances, and the interests involved must be balanced in each individual case.

> "However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."[1475]

The majority of the other recent cases in which the Court has evaluated the proportionality of interferences with the right to privacy concerned legal measures. Google Spain is notable for the fact that the CJEU has had the opportunity to balance the interest in privacy on the one hand with on the other hand, first, the economic interests of a private company, and, secondly, with the interest of other users in accessing information. The Court therefore shows that it is not only strictly protecting the rights to privacy and data protection against interferences ordered by the state, but also against interferences based on conflicting interests of other private entities.



1474 Danwitz (2015), p. 584 f. See also Michl (2017), p. 351; Prantl (2016), p. 352.
1475 CJEU Case C-131/12 *Google Spain* [2014], paragraph 81.

### vii. International Exchange of Data: Schrems and Passenger Name Records

A final group of cases that should be mentioned in this regard is that of the transfer of data internationally. Two cases should be highlighted.[1476] In the first place, this concerns the case *Schrems*,[1477] in which the CJEU invalidated the Safe Harbour Agreement under which personal data was transferred from Europe to the United States.[1478] In its judgment, the Court found clear words to describe the disproportionality of the measures of this agreement, finding the lack of proper safeguards for the protection of the rights to privacy and data protection of the data subjects to compromise the essence of these rights (article 52 (1) of the Charter).[1479] Leading up to this annihilating judgment, the Court reminded the lawmaker that "above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary".[1480] This, according to the CJEU's judgment, was not the case in the Safe Harbour Agreement.

> "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail".[1481]

The second case in this group of cases, and at the same time the newest addition to the CJEU's strict line of case law is a challenge to a planned Passenger Name Records Agreement between the European Union and Canada before the CJEU. Passenger name records is the term assigned to a set of records collected about a data

1476 See also Danwitz (2015), p. 583 f.
1477 CJEU Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* [2015].
1478 See also Emmert (2016), p. 34 ff.; Caspar (2015), p. 590 f.; Prantl (2016), p. 351; Frasher (2016), p. 14; Padova (2016), p. 139 ff.
1479 CJEU Case C-362/14 *Schrems* [2015], paragraph 94 f. See also Fuster (2016), 184 f. Dissenting *Bender* (2016), p. 118 ff. See also Chapter X below.
1480 CJEU Case C-362/14 *Schrems* [2015], paragraph 92. See also Skouris (2016), p. 1362; Petri (2015), p. 803 f.; Malgieri (2016), p. 103 ff.; Pell (2012), p. 248 ff.
1481 CJEU Case C-362/14 *Schrems* [2015], paragraph 93. See also Article 29 Working Party, Working Document 1/2016, p. 9; Petri (2015), p. 802.

subject in connection to air travel. Following the events of September 11th, 2001, the United States introduced an obligation on air carriers to submit information on their passengers to the customs authorities.[1482] Canada followed with a similar obligation.[1483] This development was to some extent mirrored and facilitated by the European Union, in the form of different legal instruments mapping out the obligations of air carriers in this context.[1484] One of these instruments was an agreement between the European Union and Canada on the transfer of passenger name records of European Union citizens to the Canadian authorities. The purpose of this exchange of data was to combat terrorism and other serious crime. Before the agreement was formally concluded, however, the European Parliament challenged the agreement by asking the Court's opinion on the compatibility of the terms of the agreement with, among other things, the rights to privacy and data protection as enshrined in articles 7 and 8 of the Charter.[1485]

The Court examined the terms of the agreement in detail, and came to the conclusion that the protection of sensitive data was not satisfactory.[1486] While the data sets that were to be transferred under the agreement did not explicitly include any categories of sensitive data, several of the categories of data it did provide to be transferred were formulated in an excessively open manner. Therefore, sensitive data might still be transferred with information under one of these open categories. This issue of a by-catch was evidently recognised by the authors of the agreement, who laid down categories of sensitive data in article 2 (e) of the agreement, and added specific rules for the processing and retention of sensitive data. The Court, however, did not accept these terms.

> "In this connection, it must be pointed out that any measure based on the premiss that one or more of the characteristics set out in Article 2(e) of the envisaged agreement may be relevant, in itself or in themselves and regardless of the individual conduct of the traveller concerned, having regard to the purpose for which PNR data is to be processed, namely combating terrorism and serious transnational crime, would infringe the rights guaranteed in Articles 7 and 8 of the Charter, read in conjunction

1482 Boehm (2009), p. 435; Petri (2008b), p. 731. See also Starosta (2010), p. 237 f.
1483 Bailey (2012), p. 215
1484 Petri (2008b), p. 732.
1485 CJEU Opinion 1/15, *PNR* [2017].
1486 See also Boehm (2009), p. 435; Boehm/De Hert (2012), p. 2.

> with Article 21 thereof. Having regard to the risk of data being processed contrary to Article 21 of the Charter, a transfer of sensitive data to Canada requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime. In this instance, however, there is no such justification.
>
> Moreover, it must be pointed out that the EU legislature has prohibited the processing of sensitive data in Article 6(4), Article 7(6) and Article 13(4) of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016[1487] on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132).
>
> Having regard to the assessments set out in the two preceding paragraphs, it must be held that Articles 7, 8 and 21 and Article 52(1) of the Charter preclude both the transfer of sensitive data to Canada and the framework negotiated by the European Union with that non-member State of the conditions concerning the use and retention of such data by the authorities of that non-member State."[1488]

Therefore, the Court did not accept the transfer of sensitive data in this context. It stated that the transfer of sensitive data must be covered by a more precise and solid justification than the general reference to the objectives of public security, terrorism, and serious crime. Therefore, in this Opinion the Court clearly continued its line of case law begun in *Digital Rights Ireland*, according to which such an objective, although being undisputedly important, cannot justify the indiscriminate interference with the rights to privacy and data protection.[1489]

The Court's assessment in *Passenger Name Records* will return in Chapter IX, particularly in the discussion of the fifth concern, in which the Court's assessment

1487 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149. Footnote added by the author.
1488 CJEU Opinion 1/15 *PNR* [2017], paragraphs 165-167.
1489 CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 51. See also Kunnert (2014), p. 781.

of the protection of sensitive data will be applied to sensitive data processed under the terms of the Anti-money laundering Directive. Furthermore, *Schrems* will play a role in Chapter X, as the CJEU notably found in this case that the essence of the right to privacy was disregarded.

**viii. Summary**

"It will be apparent from the foregoing that the concept of proportionality is a general concept used in a variety of situations, which in turn accounts for the diversity and pluriformity of the concept itself."[1490] This diversity of the application of the principle of proportionality has already become apparent in the foregoing examination of case law in a very narrow field of law, while the principle itself encompasses much more than that. The main statement that can be made about the principle of proportionality is therefore that it is a concept of singular flexibility, which serves to ensure balance and fairness in legislation and case law.

As has been seen in the examination of the case law, the development of the principle of proportionality as filled in by the CJEU has undergone significant changes in recent years. While the proportionality test applied is formally the same as ever, a shift in the balancing of interest appears to be taking place. The CJEU has had occasion in its recent case law to add significantly to the protection of the rights to privacy and data protection.[1491] It has taken the chance to speak out clearly in favour of increased protection and safeguards for the protection of these rights,[1492] and has with its decisive and general statements paved the way for challenges of other future and existing measures, too.[1493] Furthermore, all of the most recent decisions were made by the Grand Chamber, which is another sign of the great importance the Court is assigning to these questions of data protection.[1494] To quote a statement contained in a Report issued by the European Commission in the context of human rights: "the living law will ultimately be determined by the decisions of the [Court of Justice of the European Union]."[1495]



1490 Gerven (1999), p. 62.
1491 See also Streinz (2011), p. 605 f.; Danwitz (2015), p. 585.
1492 See also Leutheusser-Schnarrenberger (2016), p. 356.
1493 The arguments discussed in Chapter IX below are based on this line of case law of the CJEU as well.
1494 Skouris (2016), p. 1363. See also Fuster (2016), 184 f.
1495 European Commission (1999), p. 20. See also *Feldman's* comment on "crystal-ball gazing", Feldman (1999), p. 142.

## f. Conclusion

In the words of *Walter van Gerven*, "Proportionality remains a vague concept."[1496] Almost twenty years after his assessment, no other judgment is possible, and it is unlikely that this principle will ever be much less vague. Nor is it clear whether it would be desirable for the principle of proportionality to be more strictly defined, as the vagueness is what allows the Courts to consider each individual case in its specific circumstances and context.[1497]

In the case law of both the CJEU and the ECtHR, increased awareness of the challenges in privacy and data protection can be detected. Particularly the CJEU has taken a leading role and set a strong precedent for increased protection of those rights with its recent judgments. The cases concerning European and national data retention legislation have indicated a shift in the balancing of interests in favour of the rights to privacy and data protection, rendered very sharply due to its being repeated and clarified in *Tele2 Sverige*.

Both Courts have shown some variation and flexibility in their application of the principle of proportionality, and are likely to continue developing the content of the principle further in their future case law. Indeed, the principle of proportionality must always be applied to the facts of a specific case, and depending on the facts can bring about a different outcome at each application. The particular relevance of the context and circumstances of each individual case is the reason for the difficulty of formulating one set of criteria which would be applicable in all cases. Instead, the principle of proportionality will remain very flexible: "It has also to be said that any attempt to identify general principles risks conveying the impression that the court's approach is less nuanced and fact-sensitive than is actually the case."[1498]

The application of the principle of proportionality to existing but as yet untried measures is therefore necessarily always guesswork to some extent. Therefore, the only security in the application of this principle can be sought in following the latest judgments of the Courts, in which they have dealt with a very similar subject

1496 Gerven (1999), p. 60.
1497 Gerven (1999), p. 60.
1498 *Lord Reed and Lord Toulson* in United Kingdom Supreme Court, *Lumsdon & Ors, R (on the application of) v Legal Services Board* [2015] UKSC 41 (24 June 2015), paragraph 23.

matter. This is the reason why the data retention cases are of such importance to the assessment of the anti-money laundering measures. They will serve in this thesis as a benchmark and theoretical framework, within which the anti-money laundering measures are to be examined in order to answer the main research question.

Moreover, the series of data retention cases is far from ending. A case challenging the Montenegrin data retention rules is at present pending before the ECtHR.[1499] While the judgment in this case is still some time off, it will allow the ECtHR to recalibrate and extend its case law on the proportionality of interferences with the rights to privacy and data protection in the same way as the CJEU has done, if the ECtHR so chooses. The approach taken by the ECtHR will be anticipated with much interest.

Based on the foregoing discussion of the principle of proportionality, the following Chapter IX is dedicated to assessing the proportionality of the concrete anti-money laundering measures as contained in the European Anti-money laundering Directive.



1499 ECtHR Case of *Vanja Ćalović v. Montenegro*, Application no. 18667/11 lodged on 14 March 2011, communicated.

# PART C

# THE EVALUATION OF THE ANTI-MONEY LAUNDERING MEASURES

# Chapter IX

## The Proportionality of the Anti-Money Laundering Framework

## Outline:

a. Introduction
b. The Data Retention Cases as a Basis for Assessment
c. The Legal Basis of the Anti-money laundering Directive
d. The Level of Protection Awarded to Financial Data
e. Interferences with the Rights to Privacy and Data Protection
f. Justification: The Public Interest
    i. Justification
    ii. Critique
g. Suitability
h. Necessity and Proportionality *in Stricto Sensu*
    i. Concerns
        (1) Customer Due Diligence Measures as Measures of Mass Surveillance
        (2) No Accommodation for Professional Secrecy
        (3) Erosion of Anonymity
        (4) Lack of Transparency concerning Suspicious Transactions
        (5) No Safeguards for Sensitive Data
        (6) Lack of Respect for the Presumption of Innocence
        (7) Interference with the Freedom to Conduct a Business
        (8) Excessively wide Reporting Obligations
        (9) Requests for Information
        (10) No Notification of Data Subjects
        (11) General Lack of Procedural Transparency
        (12) Obstruction of the Right to an Effective Remedy
        (13) General Lack of Data Protection Safeguards
        (14) Excessive Retention Periods
        (15) Access to Data by Tax Authorities
        (16) Lack of Respect for the Principle of Purpose Limitation
        (17) Additional Proposed Rules

## a. Introduction

In the previous chapters, some of the conflicts between the provisions of the Anti-money laundering Directive and the fundamental rights to privacy and data protection have already been alluded to. A detailed discussion on privacy and identity issues in the framework and in particular in the Anti-money laundering Directive naturally begs the question if the Directive, with all its flaws, can still be deemed proportional and compatible with the fundamental rights to privacy and data protection under European Law.[1500] This question is at once the main research question, which is now to be answered in this present chapter.

The subject of this chapter is to assess the balance between the conflicting interests of society in both the effective prevention, detection, and investigation of serious crimes on the one hand, and in the protection of the personal data and privacy of the population on the other hand.[1501] It is important to note that both interests are public interests, i.e. interests of society as a whole. However, as will be seen in the following sections, the rules designed in order to serve the public interest in public security are to the detriment of the other public interest in respecting the privacy of the population. Particularly the use of electronic data processing for the detection of crime has a big negative impact on the privacy of the population.[1502] In addition, covert processing of the data, and the inclusion of the personal data of individual with no or only an indirect connection to a crime or a criminal may make the intrusions into the privacy rights of the population particularly serious.[1503]

In order to ensure that due respect is paid to both conflicting interests of society in cases such as this, where the introduction of a measure in the public interest brings with it the detriment of another public interest, a balance must be struck between the two interests. The measure is proportional only when the benefits and costs of a measure are balanced properly. The structure of this balancing act is determined by the principle of proportinaltiy, which was already described in the previous Chapter VIII. The purpose of this present chapter is then to apply

1500 In the words of Diderot (1746), p. 140, "Le scepticisme est donc le premier pas vers la vérité."
1501 See also Krings (2015), p. 168; Raab (2014), p. 42.
1502 Glaessner/Kellermann/McNevin (2002), p. 18
1503 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 58. See also Milaj/Kaiser (2017), p. 121 ff.

the principle of proportionality to the case of the fourth and where applicable, the proposed fifth Anti-money laundering Directives[1504] in order to assess the balance between the public interests involved. At the same time this chapter will answer the main research question of this thesis, namely whether the anti-money laundering framework currently in place respects fundamental rights and the principle of proportionality.

This chapter is organised according to the following system: In the beginning (b), the case law concerning data retention is to be recalled, as it largely serves as a benchmark for comparison. This section will show the similarities in the measures of the instruments of the Data retention Directive and the Anti-money laundering Directive. In this context, a few words should also be said about the legal basis of the two Directives (c). The first data retention case, Ireland v. Parliament and Council of 2009,[1505] concerned the legal basis of the Data retention Directive, and a comparison between this Directive and the Anti-money laundering Directive naturally prompts some questions concerning the legal basis of the Anti-money laundering Directive as well. In the following section (d), the protection of financial data will be examined. This section will show that financial data and the information that can be gathered from an analysis of financial data are comparable in sensitivity to the communication data processed under the Data Retention Directive. After these initial comparative sections, the detailed examination of the proportionality of the Anti-money laundering Directive will begin. Following the structure chosen by the CJEU when it examines challenges to legislation based on proportionality, the interferences with the rights to privacy and data protection by the anti-money laundering measures are going to be enumerated (e). Section (f) is concerned with the public interest justification of these measures, and will also contain a critique of this justification. Section (g) is going to examine the first condition of the proportionality test, which is the suitability of the measures to reach the public interest objective in question. Section (h), the bulkiest section in this thesis, will examine the second and third conditions of the proportionality test, namely necessity and proportionality *in stricto sensu*. It will turn to a detailed discussion of the criticisms that can be levelled against the measures of the Anti-



1504 Please note that unless stated otherwise, the text of the fifth Presidency compromise 15605/16 of 19 December 2016 was used.
1505 CJEU Case C-301/06, *Ireland v European Parliament and Council of the European Union* [2009].

money laundering Directive. This section contains seventeen concerns[1506] which are raised by the measures of the Directive, and based on which the assessment of the proportionality will be carried out in section (i). Finally, as an epilogue to this chapter after the main research question was answered, section (j) examines the level of protection of one's privacy and personal data that can be achieved by using alternative transaction systems.

## b. The Data Retention Cases as a Basis for Assessment

Existing case law is the main guide in the review of the proportionality of a certain measure.[1507] The case law of the CJEU, the ECtHR and the highest courts of the Member States is immensely useful in bringing the proportionality principle to life and in order to assess the proportionality of any given measure.[1508] While the proportionality case law of the CJEU and of the ECtHR is made up of a patchwork of cases in which the courts created ever finer distinctions and an ever more solid basis for its proportionality assessment, naturally recent cases concerning a similar subject matter as the measure under review are most useful to refer to.

Therefore, the assessment of the proportionality of the measures of the Anti-money laundering Directive can best be based on the CJEU's case law concerning the Data retention Directive,[1509] which is at once similar in subject matter to the Anti-money laundering Directive and recent in the sense that the data retention cases have been decided within less than a decade from the time of writing. The Data retention Directive[1510] was a European directive regulating the retention of connection data ('metadata')[1511] by telecommunications services providers for a period between six months and two years, in order to facilitate access to this data by law enforcement agencies in the event of an investigation into serious crime.

1506 These concerns were already mentioned at different points in this thesis. The discussion of the concerns started in Chapter II section (g).
1507 See also sections (c) and (e) of Chapter VIII above.
1508 Manger-Nestler/Noack (2013), p. 505 f.
1509 See also EDPS Opinion 1/2017, p. 11 f.
1510 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.
1511 Article 29 Working Party, Opinion 4/2014, p. 4. See also Korff (2014), p. 115; Maras (2012), p. 66.

Three legal battles were fought before the CJEU about the Data retention Directive. The first case, *Ireland vs. Parliament and Council* of 2009,[1512] was an action for annulment of the Directive based on the claim that the legal used for this Directive could not support it, as the content of the Directive was not related as closely to the single market as to the prevention, investigation, detection or prosecution of criminal offences.[1513] The CJEU, however, did not agree with the arguments of Ireland and Slovakia in this case and the Directive was allowed to remain in existence.

Five years later, in a landmark decision in 2014, the CJEU did invalidate the Data retention Directive in a new proceeding. The serious infringements of the citizens' rights to privacy and data protection caused by the measures contained in the Directive were deemed disproportional to the intended aim of fighting serious crime, and to the projected benefits of the retention of the data.[1514]

However, although the Directive was thus invalidated, national laws stipulating the retention of data were kept in place in several Member States.[1515] In a third decision in December 2016, the CJEU was called upon to rule on the compatibility of national data retention laws with European legislation.[1516] In this decision, the national data retention laws were measured by the yardstick of article 15 (1) of the e-Privacy Directive 2002/58,[1517] which allows retention of data only on the condition that the retention is proportional, serves specific public interests, and that data is stored only for a limited period of time. This article, read in conjunction with the Charter and respecting the principle of proportionality, was interpreted by the Court to preclude excessive data retention laws also on national level. In *Tele2 Sverige*, the Court therefore confirmed its ruling in *Digital Rights Ireland*,



1512 CJEU Case C-301/06, *Ireland v European Parliament and Council of the European Union* [2009]

1513 Kahler (2008), p. 449 f.

1514 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (C-293/12) *v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung* (C-594/12) *and Others* [2014]. See also Goemans/Dumortier (2003), p. 167 f.

1515 See for a discussion of the French system Maxwell (2014), p. 5 ff.; the Italian system in Resta (2014), p. 16 f.

1516 CJEU Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016].

1517 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

and extended the application of its strict line of case law to data retention laws on the national level.[1518]

In principle, the CJEU is the only authority on the proportionality of secondary European Union laws, but the Data retention Directive has caused a great stir also on Member State level. Before the CJEU handed down its decision, the laws implementing the Directive were already being challenged and tested in several Member States as to their compatibility with the national constitutions. The most notable national decision was the invalidation of the legal amendments implementing the Data retention Directive into German law by the *Bundesverfassungsgericht*, the German Constitutional Court (BVerfG).[1519]

As the structure of the examination of an interference with human rights is much the same in both systems, the two judgments *Digital Rights Ireland* and *Tele2 Sverige*, and the judgment of the BVerfG lend themselves particularly well for comparison. Indeed, "[t]he concept of proportionality is most fully developed within German law",[1520] and therefore German law might be the best option to supplement the discussion. In addition, the German Constitutional Court is generally regarded as having assumed the leading role in the development of the rights to privacy and data protection,[1521] and its judgments are internationally regarded as being of great authority. The CJEU and the BVerfG in their data retention cases reached much the same conclusion, but each court took a slightly different route to this result. The decision of the BVerfG is especially notable as to the novel holistic approach it introduces with regard to surveillance measures,[1522] as well as its detailed discussion of the balance between the retention and access of communications data and the rights of the concerned individuals.

Thus, where the Anti-money laundering Directive introduces the surveillance, access, and the retention of financial transactions, the Data retention Directive introduced retention and access of communication data. The crucial common

1518 It should be pointed out that the specific circumstances of this case allowed for this review. Not all national laws are subject to review by the CJEU.
1519 BVerfG, 1 BvR 256/08 [2010]. The original German text has been used for the purposes of this thesis, translated by the author.
1520 Craig/De Búrca (2015), p. 551; Manger-Nestler/Noack (2013), p. 505; Jacobs (1999), p. 1 f.
1521 Skouris (2016), p. 1364.
1522 This approach will be subject to some discussion in the following Chapter X.

point is that telecommunication services providers and financial services providers are private legal persons, which participate in the European Single Market, and which have a very elaborate collection of customer data for their own purposes already.[1523] This sophisticated data set is built, for instance, by telecommunications services providers in order to be able to bill their customers accurately for their connections. A similar system is built by banks in order to provide their (online) banking services to customers, or by credit card companies for billing purposes and similar tasks.[1524] The set of data therefore exists already, and all the Directive does is compel service providers to monitor this data not only in its own interest, but also on behalf of law enforcement agencies in order to detect movements which may be connected to money laundering or terrorist financing. Furthermore, service providers are obliged to retain the data for a longer period of time than they would normally retain it in their own interests. Finally, the costs remain with the service provider and are generally passed on the customer.

The Data retention Directive naturally covered a very different subject matter than the Anti-money laundering Directive does, and the approaches chosen in the two directives are also different. In particular, the two directives differed in the way in which the authorities could take note of data concerning a data subject. The Data retention Directive provided for a 'pull'-system, in which the authorities would initiate the exchange of data and the service provider was obliged to comply with the authorities' requests. The Anti-money laundering Directive is mainly constructed around a 'push'-system, in which the obliged entities must transmit data on their own initiative to the FIU. However, the Anti-money laundering Directive also provides for a form of a 'pull-system', in the sense that FIUs can request information from obliged entities.[1525] This option of the FIU to request information from obliged entities is furthermore gaining in importance and is to be extended with the proposed fifth Anti-money laundering Directive. In addition, in matters concerning the surveillance of the population, the grand scale of the surveillance, and the risks attached to monitoring the population at this scale, the two directives are very much alike. Applying the findings of the CJEU and the BVerfG in the data retention cases to the Anti-money laundering Directive is



1523 See also Korff (2014), p. 85; Gurlit (2010), p. 1040.
1524 Eichler/Weichert (2011), p. 202 f.
1525 This option is gaining in importance in the draft to the fifth Anti-money laundering Directive, as the Commission's explanatory document to the first draft of the proposed fifth Anti-money laundering Directive shows, see COM(2016) 450 final, p. 13 f.

therefore the most accurate way to determine the proportionality of the measures in question.

## c. The Legal Basis of the Anti-money laundering Directive

Before going into details concerning the content of the Anti-money laundering Directive, one formal aspect of its genesis should be examined briefly. While this chapter is in principle solely concerned with the material contents of the Directive, its formal aspects also lend themselves to a comparison with the Data retention Directive.

All legislative and executive powers of the European Union are limited by the three principles of conferral, subsidiarity, and proportionality enshrined in article 5 of the Treaty on the European Union (TEU).[1526] The principle of conferral is a limit to the competences of the Union by restricting the powers of the European Union to the amount and extent of the competences conferred to it by the Member States through the Treaties. In contrast to the Member States themselves, the Union does not have the competence to acquire new competences in any other way than through a treaty between the Member States.[1527]

The legal basis of any act of the Community is of great importance.[1528] There are numerous legal bases contained in European Union primary law, which grant the European Union the power to pass directives, regulations, or other forms of legal act in order to regulate a certain area of law. While legal bases in European Union law are typically formulated in a rather open way, they are also subject to material constraints and procedural norms designed to allow Member States to intervene in order to protect their sovereignty.[1529] In cases where it is disputed that the correct legal basis was used for a certain legal act, an action for annulment of that legal act can be brought to the CJEU.

1526 See Chapter VIII above.
1527 Trstenjak/Beysen (2012), p. 266.
1528 Ziebarth (2009), p. 27.
1529 *Bradley* in Barnard/Peers (2014), p. 106. See also Jellinek (1914), p. 435; Gietl/Tomasic (2008), p. 796 f.

Just such an action for annulment was begun before the Court in 2006 by Ireland against the Data retention Directive.[1530] As this Chapter compares the different aspects of the Anti-money laundering Directive so closely to the Data retention Directive, this particular aspect should also be examined briefly. In *Ireland vs. Parliament and Council*, Ireland argued that the Data retention Directive should not have been based on article 95 TEC (now article 114 TFEU), as that legal basis concerns the internal market.[1531] Ireland brought forward that "the sole objective or, at least, the main or predominant objective of that directive is to facilitate the investigation, detection and prosecution of crime, including terrorism."[1532] Ireland thus argued that the Directive's primary aim was not to harmonize the internal market but rather to facilitate investigations by law enforcement agencies into serious crimes, and that therefore, article 95 TEC should not have been used as a legal basis for this particular Directive.

The case against the legal basis of the Data retention Directive is interesting because it allows some parallels to be drawn to the Anti-money laundering Directive. The Anti-money laundering Directive is equally based on article 114 TFEU, and its predecessors were based on article 95 TEC, presupposing a close connection between the Directive and the internal market. The criticisms about the choice of legal basis for the Data retention Directive also apply to the Anti-money laundering Directive. Although the recitals of the Anti-money laundering Directive mention the internal market several times, the substantive content of the Directive appears to concern primarily the prevention of money laundering and terrorist financing.

The concerns about the validity of the legal basis for the Data retention Directive were not shared by the Court in this case. The Court focused on the effect of the Directive of creating a level playing field among telecommunications services providers within the European Union. The Court considered that the terrorist attacks of the years before the adoption of the Directive have caused Member States to introduce measures of data retention as "effective means for the detection



1530 CJEU Case C-301/06, *Ireland vs. Parliament and Council* [2009].
1531 See also Article 29 Working Party Opinion 14/2011, p. 8; Bizer (2007b), p. 587; Gietl/Tomasic (2008), p. 796 f.
1532 CJEU Case C-301/06, *Ireland vs. Parliament and Council* [2009], paragraph 28. See also Ziebarth (2009), p. 27.

and prevention of crimes".[1533] Furthermore, the Court assumes that those Member States which had not yet introduced laws for the retention of telecommunications data would do so in the future.[1534] The different applications of the national data retention rules would be "liable to have a direct impact on the functioning of the internal market",[1535] which made action on the European level necessary and justified the use of article 95 TEC as a legal basis for the Directive.

While the reasoning of the Court may justify the use of article 95 TEC, it does appears rather artificial and constructed when the actual content of the Directive is brought back to mind.[1536] It rather appears that the positive impact of the harmonization of data retention rules across Europe is only incidental to the substantive rules for the purpose of investigating, detecting and prosecuting crime.

In this context, it should be pointed out that the Data retention Directive was adopted under the pillar structure, which is no longer applicable. In contrast, the fourth Anti-money laundering Directive was adopted on the legal basis of Article 114 TFEU. Therefore, the findings of the Court in *Ireland vs. Parliament and Council* can no longer be directly applied to the Anti-money laundering Directive. It is not entirely clear how the Court would respond to a challenge to the legal basis under these changed circumstances. Therefore, although the subject matter of this chapter is an assessment of the proportionality of the measures of the Directive rather than of the validity of the legal basis, the weakness of the legal basis is still an important issue. It serves to illustrate that the Directive not only contains measures which are problematic from the perspective of human rights, but also stands on an exceedingly shaky legal basis.

## d. The Level of Protection Awarded to Financial Data

The Data retention Directive concerned communication data, which enjoys particular protection not only under the rights to privacy and data protection

1533 CJEU Case C-301/06, *Ireland vs. Parliament and Council* [2009], paragraph 67. It should be pointed out that the effectiveness of this means is not undisputed, as was brought forward as an argument against the proportionality of the Data retention Directive in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 50.
1534 CJEU Case C-301/06, *Ireland vs. Parliament and Council* [2009], paragraph 70.
1535 CJEU Case C-301/06, *Ireland vs. Parliament and Council* [2009], paragraph 71.
1536 Ziebarth (2009), p. 27.

but also the freedom of expression (article 11 of the Charter). Financial data does not enjoy such explicit protection. This, however, certainly does not imply that a lower level of protection should be applied to financial data. On the contrary, a customer's financial transaction data has a similarly revelatory character as communications metadata, in the sense that it allows very intimate insights into a person's daily life and habits.[1537] A high level of protection for financial data is therefore necessary in order to protect data subjects from risks concerning their privacy and personal data.

There are different traditions in the different Member States about how highly people value their financial privacy, and different regulatory responses reflect these traditions.[1538] On the one hand, there are some countries in which financial privacy is an important principle, with banking secrecy a highly protected value in law.[1539] On the other hand, there are countries which value financial transparency more highly, which is, for example, reflected in the opening of tax data to the public.[1540] However, the countries in which there is greater financial transparency generally only lay limited sets of data open to the public, which are related to the income of a person. In this case, financial transparency and the greater possibilities for control can lead to increased income equality between men and women, fairer taxation, and prevention of tax fraud.[1541]

How an individual chooses to spend their money is not generally laid open to the public anywhere. Indeed, the protection of the customer's privacy used to be a very high value in the financial sector.[1542] Until recently,[1543] the work of credit institutions and financial institutions in most Member States of the European Union was shaped to a great degree by banking secrecy.[1544] Banking secrecy described on the one hand the confidentiality of the customer's financial information, which



1537 See also Chapter V above.
1538 Glaessner/Kellermann/McNevin (2002), p. 18. See also Heine (2017), p. 368 ff.
1539 See however Schmidt/Ruckes (2017), p. 474 f.
1540 EDPS Opinion 1/2017, p. 13. See also the discussion of the proportionality assessment of the CJEU in the case *Schecke* in Chapter VIII above, CJEU Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR* (C-92/09) *and Hartmut Eifert* (C-93/09) *v Land Hessen* [2010].
1541 COM (2016) 451 final, p. 3. See also ECHR Case of *Wypych v. Poland* [2005]. See also, however, EDPS Opinion 1/2017, p. 13.
1542 See also Ahrens (2015), p. 1083.
1543 Schmidt/Ruckes (2017), p. 474 f. Banking secrecy laws are by now largely abolished or hollowed out throughout the European Union.
1544 See in this context also Chapter V (d) above.

was a major obligation in the relationship between the bank and the customer, and on the other hand it developed an external dimension by allowing the bank to deny information to third parties,[1545] including to government authorities.[1546] In principle, the banking secrecy rules could only be overruled by the applicable procedures, for instance in the presence of a judicial warrant.[1547]

Information on a customer's financial choices and transactions were thus in principle protected. There are very good reasons for this protection. Not only is a person's transaction history a reflection of a series of individual decisions depending on an individual's personal preferences, habits, and needs, but it can also allow intimate views of a person's private life. As has already been discussed above, a person's spending can allow immediate reflections on a person's daily habits and private life.[1548] A person's transaction history may contain donations which allow conclusions on this person's political or religious beliefs. It may contain payments at institutions, shops, or entertainment venues which are connected to the LGBT community or are otherwise connected to a person's sex life. An individual may pay high medical bills. All those things directly concern this individual's immediate private life and fall within the categories of sensitive data,[1549] and should therefore certainly not be disclosed to the public at large or the law enforcement authorities.

Revelation of such information might indeed cause great problems for an individual, depending on to which institutions and persons this information is revealed. People will generally want to choose to whom they reveal intimate information about themselves, such as for example their sexual preference. Even in countries where the non-discrimination of homosexuality is guaranteed by law,[1550] homosexuals do face ostracism and discrimination. In other areas in the world, homosexuality is still severely punished by law. If, therefore, as in one of the examples above, financial transactions can relate to and reveal an individual's sexual preference, that information must be especially protected. The lawmaker has recognized the problems which can be caused to data subjects if such data were

1545 See however CJEU Case C-580/13, *Coty Germany GmbH v Stadtsparkasse Magdeburg* [2015].
1546 Tolani (2007), p. 275. See also Heine (2017), p. 368 ff.; Schmidt/Ruckes (2014), p. 653.
1547 See also Roßnagel/Bedner/Knopp (2009), 540.
1548 See also Chapter V above.
1549 Article 29 Working Party Opinion 14/2011, p. 26; EDPS (2015), p. 7.
1550 As is the case in the European Union: Discrimination on a number of grounds, among others sexual orientation, is prohibited by Article 21 (1) of the Charter.

not treated with perfect care.[1551] The GDPR is thus also very clear in forbidding the processing of those categories of data, except where the exceptions of article 9 (2) apply, which, however, must be interpreted narrowly.

The data retention judgment of the CJEU observes exactly this looming danger, that the data gleaned from the customers' communication metadata records may reveal conclusive details of the customers' private lives.[1552]

> "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[1553]

Such a revelatory character is not exclusively reserved to the telecommunications data of individuals. Any customer's private bank account will contain references to all of those aspects of the customer's private life mentioned by the CJEU, in the form of financial transactions which include time stamps, the identity of the recipient, and the periodical or non-recurring character of the transaction. The information which can be gleaned from a bank customer's transaction history of just a few weeks or months may reveal very intimate details of a person's life and daily habits, including details belonging to the realm of sensitive information, to which special protection is awarded by law.[1554]

Recognizing those implications, the need for a high protection of financial data becomes evident. Therefore, the fact that the Data retention Directive concerned communications data should not stand in the way of the application of the findings of the CJEU to the Anti-money laundering Directive. On the contrary, the necessity of a high level of protection for financial data is emphasised by



1551 See also European Economic and Social Committee 13666/16, p. 7. The EESC shows itself mildly concerned about "the improper use by the competent authorities of a large volume of sensitive information", but does not draw quite the same connections as are made here.
1552 Article 29 Working Party, Opinion 4/2014, p. 4. See also EDPS (2015), p. 7; Korff (2014), p. 115; Feiler (2010), p. 17; Katzenbeisser (2016), p. 99; Pimenidis/Kosta (2008), p. 95.
1553 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 27. See also Pimenidis/Kosta (2008), p. 95; Pfitzmann/Köpsell (2009), p. 543.
1554 Article 29 Working Party Opinion 14/2011, p. 7.

the similarity of the potential impact and the revelatory character of the data. Considering the similarity of the measures contained in the two directives as outlined above in Section (b) and the necessity of a high level of protection of both communications data and financial data, the CJEU's case law on data retention is not only relevant to but also authoritative with respect to the application to the Anti-money laundering Directive.

## e. Interferences with the Rights to Privacy and Data Protection

The measures introduced by the Anti-money laundering Directive have been discussed in great detail in earlier chapters.[1555] What has so far been omitted is a clear classification of those measures in terms of interferences with the rights to privacy and data protection as defined and guaranteed in articles 7 and 8 of the Charter of Fundamental Rights.

The CJEU in its case law on proportionality usually follows roughly the same structure. It begins by establishing in what ways, if any, the contested measures interfere with the fundamental rights or freedoms in question. In a following step, it considers the legitimate aim which is given as a justification for these measures. Only after those two steps does it turn to an assessment of the proportionality of the contested measures with regard to this legitimate aim. This structure is going to be applied here, not only because of the authority of the CJEU in this regard and because there isf simply no other accepted scheme for the assessment of the proportionality of directives, but also because the structure is very logical: The conflict between the law and fundamental rights is manifested in the interferences of a measure with fundamental rights. Any interference, once established, must be justifiable with a legitimate public interest. Finally, the proportionality of the interference is assessed. The assessment of the proportionality of the Anti-money laundering Directive to be made in this Chapter therefore starts here with an enumeration of the interferences of the measures of the Anti-money laundering Directive with the rights to privacy and data protection in the present section (e), an examination of the justification in section (f) and finally the examination of the proportionality in sections (g) and (h).

1555 This concerns particularly Chapter II.

The CJEU has not yet developed a uniform definition of what an interference constitutes.[1556] However, the case law of both the CJEU and the ECtHR in the field of privacy and data protection is ample, and both courts have in the past interpreted the term interference broadly.[1557] In addition, most of the interferences that can be identified in the case of the Anti-money laundering Directive are sufficiently similar to interferences discussed in earlier case law and/or recognised in literature to allow a clear classification.[1558]

All of the data processing mechanisms of the Anti-money laundering Directive have already been described in detail in Chapter II. Roughly, this concerns the collection of personal data following from the duty to identify all customers, the surveillance of transactions resulting from the duty to monitor, the exchange of personal data when an obliged entity complies with its reporting duty or with an information request by the FIU, and the storage of data due to the obligatory data retention. The data processing based on the four main obligations falling on obliged entities result in the following interferences.

In the first place, data is being collected about the customer.[1559] That covers information about the customer's identity, in particular his name, address, phone number, and other personal information, including in most cases a photocopy of the customer's identity card or passport, pursuant to Article 13 of the Anti-money laundering Directive. Furthermore, information is collected about the customer's transactions: All financial transactions carried out by the financial services provider on behalf of the customer are thus recorded and archived by the financial services provider. Depending on the nature of the service provider, that record can be limited to a single transaction, as in the case of a lawyer or notary, or to thousands of transactions, as in the case of an active bank account. This collection of data constitutes an interference with the rights to data protection and privacy.[1560]



1556 Manger-Nestler/Noack (2013), p. 505. See also Gavison (1984), p. 357 f.
1557 Manger-Nestler/Noack (2013), p. 505; Kielmansegg Graf (2008), p. 24 f.; Böszörmenyi/Schweighofer (2015), p. 71 f.
1558 The literature largely concerns data retention, but the interferences are comparable due to the similarity of the data processing operations made mandatory by both Directives.
1559 Kunnert (2014), p. 775.
1560 Article 29 Working Party, Working Document 1/2016, p. 6.

In the second place, the data is further processed by the financial services provider, by continuously monitoring all transactions for possible suspicious transactions pursuant to Article 13 (1) (d) of the Anti-money laundering Directive.[1561] This processing is a second interference with the rights to privacy and data protection.[1562]

In the third place, in cases where a red flag was raised by any transaction, the financial services provider is obliged to report that transaction to the financial intelligence unit. The suspicious transaction report is accompanied by all relevant information about the customer and the transaction. The customer is not notified of this report (article 31 (1) 4AMLD).[1563] It should be added that requests for information from FIUs directed to obliged entities also play a big role, which is to be expanded with the introduction of the amended rules of the proposed fifth Anti-money laundering Directive. The Commission states in its accompanying explanation to the first draft that FIUs must be placed in a position to request information from any obliged entity, or even to be granted direct access to information retained by those entities.[1564] Therefore, the amendments of the measures by the fifth Anti-money laundering Directive will likely increase the amount of requests for information from FIUs. The transmission both in the shape of sending a suspicious transaction report and in the shape of complying with a request for information constitutes a further interference.[1565]

In the fourth place, it should be noted that the proposed fifth Anti-money laundering Directive is also intended to include the introduction of a central register of bank account holders in each Member State. The Commission explains that "FIUs and other AML/CFT authorities […] must have efficient means to identify all bank and payment accounts belonging to one person through a centralised automated search query."[1566] The Directive would thus demand the introduction of central registers containing information on each bank account held in a credit institution in a Member State, storing personal information on the holder of the account and accessible to the competent authorities in that State. The inclusion of personal information in such a register and the access of that information constitutes an interference.[1567]

1561 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 36.
1562 Article 29 Working Party, Working Document 1/2016, p. 6; Dittrich/Trinkaus (1998), p. 347.
1563 See in this context also Boehm/De Hert (2012), p. 4.
1564 COM (2016) 450 final, p. 14.
1565 Böszörmenyi/Schweighofer (2015), p. 72.
1566 COM (2016) 450 final, p. 14. See also Maidorn (2006), p. 3753; Kutzner (2006), p. 643 f.
1567 Article 29 Working Party, Working Document 1/2016, p. 6.

The same is true for the potential installation of databases containing information on users of virtual currencies which the Commission has been exploring as an option.[1568] Such databases would be created in order to be able to identify the holders of wallet addresses tracked in the blockchain. The implementation of such databases would constitute another interference.[1569]

In the fifth and final place, the customer's identity record as well as the full transaction history of the customer with the financial services provider is to be retained for five years after the end of the business relationship, a term which can be extended under certain circumstances to ten years. In the words of the CJEU in the *Digital Rights Ireland* judgment, such retention "constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter."[1570]

The sum of those interferences makes the infringements of the rights to privacy and data protection singularly serious. The interferences of the measures in the Anti-money laundering Directive in many instances very much resemble the interferences of the measures in the Data retention Directive, which were so excoriated by both the BVerfG and the CJEU.[1571] The courts both identified the danger that the retention of telecommunications data and access to this data by law enforcement agencies without the knowledge of the customers concerned could have a very negative impact on society as a whole. The BVerfG identified the concern that "the storage of telecommunications traffic data without cause is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas."[1572] This same sentiment was echoed by the CJEU in its subsequent judgment, stating that "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[1573]



1568 COM (2016) 450 final, p. 38 f.
1569 Rückert (2016), p. 18.
1570 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 34; see however BVerfG, 1 BvR 256/08 [2010], paragraph 313. See also Böszörmenyi/Schweighofer (2015), p. 72.
1571 See also Feiler (2010), p. 8.
1572 BVerfG, 1 BvR 256/08 [2010], paragraph 212. See also Nicoll (2003), p. 116; Leutheusser-Schnarrenberger (2014), p. 591. See however Koshan (2016), p. 168.
1573 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 37. See also Dix/Petri (2009), p. 534.

## f. Justification: The Public Interest

### i. Justification

Under European Law, any measure taken by the institutions, and any infringement of the four fundamental freedoms or of any other rights granted to the citizens and legal persons in the European Union, must be proportional to the aim which is to be achieved by the measure in question.[1574] A measure is only proportional if it fulfils the following three conditions. In the first place, "the principle of proportionality requires that measures adopted by European Union institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question."[1575] On a second level, "when there is a choice between several appropriate measures recourse must be had to the least onerous".[1576] Finally, on a third level, "the disadvantages caused must not be disproportionate to the aims pursued".[1577]

Proportionality is therefore a complex reckoning to find the best cost-benefit ratio, i.e. a situation in which an objective in the public interest can be achieved as well as possible, while the freedoms and rights of individuals are infringed in a minimum degree. Such a calculation is not always easy, and the value of a certain public interest in relation to a certain individual right or freedom are not always straightforward.

Public interests exist in all kinds of different shapes. The public interest ground in question in this case is the fight against serious crime.[1578] Recital 42 of Directive 2015/849 states that "The fight against money laundering and terrorist financing is recognized as an important public interest ground by all Member States."[1579] This is repeated in article 43 4AMLD once again, specifically to justify the processing of information as prescribed by the Directive: "The processing of personal data on the basis of this directive for the purpose of the prevention of money laundering

1574 See Chapter VIII above.
1575 CJEU Case C-343/09 *Afton Chemical* [2010], paragraph 45, and CJEU Joined Cases C-581/10 and C-629/10 *Nelson* [2012], paragraph 71, quoted by *Hofmann* in Barnard/Peers (2014), p. 204. See also Schröder (2016), p. 642.
1576 CJEU Case C-343/09 *Afton Chemical* [2010], paragraph 45, and Joined Cases C-581/10 and C-629/10 *Nelson* [2012], paragraph 71, quoted by *Hofmann* in Barnard/Peers (2014), p. 204.
1577 CJEU Case C-343/09 *Afton Chemical* [2010], paragraph 45, and Joined Cases C-581/10 and C-629/10 *Nelson* [2012], paragraph 71, quoted by *Hofmann* in Barnard/Peers (2014), p. 204.
1578 See also Article 29 Working Party Opinion 14/2011, p. 8.
1579 See also European Economic and Social Committee 13666/16, p. 3.

and terrorist financing as referred to in article 1 shall be considered to be a matter of public interest under Directive 95/46/EC."

The same justification was used for the Data retention Directive. The Court summarized that

> "the material objective of that directive is, as follows from Article 1 (1) thereof, to ensure that the data are available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security."[1580]

In more detail, the Court clarifies that both the fight against terrorism "in order to maintain international peace and security" as well as the fight against serious crime are each objectives of the general interest in their own rights.[1581] In addition, the Court clarifies that the Charter in article 6 enshrines a right of the European population to security.[1582]

The Anti-money laundering Directive is very similar in this regard to the Data retention Directive. However, different opinions on this assessment of the objective of general interest are certainly valid. The fight against money laundering in particular is a process which was not exactly driven by the Member States themselves.

A related interest is that of curbing terrorism by fighting the financing of terrorism. Since the events of September 11th, 2001 and the subsequent series of attacks in major European cities, the fight against terrorism has become a policy priority and has been used to introduce far-reaching intrusions into the fundamental rights and freedoms of citizens.[1583] The rights which are affected most often and to the strongest degree are those of privacy and data protection. However,



1580 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 41.
1581 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 42. See also Böszörmenyi/Schweighofer (2015), p. 72.
1582 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 42. See, however, Article 29 Working Party, Opinion 4/2014, p. 6.
1583 See also FATF Money or Value Transfer Services (2016), p. 18.

while the courts certainly accept that legislators must take countermeasures to the threat of terrorism,[1584] they are strict in their assessment of the compatibility of those measures with human rights guarantees. As has been shown in Chapter VIII above, the recent case law at least of the CJEU is making clear that even an important policy objective such as that of fighting terrorism cannot justify massive data collections such as those carried out pursuant, for instance, the Data retention Directive.[1585] The public interest justification of fighting terrorism should therefore be regarded as a potent justification, but certainly not as an end that can justify all means.[1586]

In addition to the public interest in fighting serious crime and terrorism, however, other policy considerations also play a part in the justification of the measures of the Anti-money laundering Directive. In particular, the fight against tax evasion and tax avoidance plays a role in anti-money laundering. While in the fourth Anti-money laundering Directive, tax crimes can only be a predicate offence to money laundering, this link is strengthened with the most recent legislative activity.[1587] The Commission's proposal therefore also mentions "enhanced corporate transparency" as a justification for the measures of the fifth Anti-money laundering Directive.[1588] In the words of the Commission, "[t]his proposal seeks to prevent the large-scale concealment of funds which can hinder the effective fight against financial crime, and to ensure enhanced corporate transparency so that true beneficial owners of companies or other legal arrangements cannot hide behind undisclosed identities."[1589]

In a communication released on the same day as the proposal for a fifth Anti-money laundering Directive, the Commission elaborates on this second justification, and stresses the lack of transparency in tax matters as one reason for the revision of the fourth Anti-money laundering Directive.[1590] The Commission goes on to state that

1584 See ECtHR Case of *Klass and Others v. Germany* [1978], paragraph 48.
1585 CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014], paragraph 51. See also Skouris (2016), p. 1364.
1586 Korff (2014), p. 108.
1587 EDPS Opinion 1/2017, p. 8; Kaetzler (2008), p. 180.
1588 COM (2016) 450 final, p. 2.
1589 COM (2016) 450 final, p. 2.
1590 COM (2016) 451 final, p. 5 f.

> "tax authorities must be given access to the data provided under the EU's anti-money laundering rules, notably customer due diligence information and the information in their national beneficial ownership registries, in order to perform their tasks and not only in the context of the fight against money laundering and terrorist financing."[1591]

The move towards multiple policy goals is therefore evident in this statement. While earlier, the fight against serious crime was cited as the only major justification for the Directive, the Anti-money laundering Directive will be integrated into more than one policy field in the future.

**ii. Critique**

This justification that the Directive will aid the fight against money laundering and terrorist financing is, however, not entirely undisputed. Money Laundering cannot be separated from the underlying predicate offence by which the funds which are to be laundered were generated.[1592] The nature of predicate offences ranges widely, drug-related offences and other types of organized crime, corruption, and fraud being the classical predicate offences.

The crime of money laundering is a relatively new crime, which has been hotly debated before it was finally recognized as a crime in every Member State. Notably Germany was rather late to introduce Money Laundering as a specific crime into its criminal code in 1992,[1593] after several years of considerable political pressure from the United States.[1594] The value of the new provisions was not apparent to many scholars at the time it was introduced. Even now, money laundering is not a primary interest in many police investigations, especially in investigations into drug-related organized crime, to which money laundering is often most closely connected to. *Soudijn* soberly summarizes that "In reality, financial leads are often thought of as a side-line during drug investigations."[1595] The logic behind this strategy is likely to bundle resources in order to fight the predicate offences to



1591 COM (2016) 451 final, p. 6.
1592 Article 29 Working Party, Opinion 14/2011, p. 16 f.
1593 The Netherlands did not make money laundering a fully-fledged criminal offence until 2001. See Oerlemans et al. (2016), p. 37.
1594 For a critical contemporary analysis of the new crime, see Arzt (1990), p. 1 ff. Interestingly, money laundering had only become a separate criminal offence in the United States relatively recently, too, having been introduced in 1986. See Gouvin (2003), p. 967.
1595 Soudijn (2014), p. 200. See also Lambert (2002), p. 367.

money laundering, rather than the financial crime itself. This process is further reinforced by sourcing investigations into money laundering out to the FIUs. The low priority assigned to money laundering investigations by the police is starkly at odds with the extensive powers and resources spent on FIUs and their investigations.

That money laundering itself should be classified as a serious crime is not self-evident.[1596] That the perpetrator of the predicate offence wishes to use the funds generated by that offence goes without saying, it is indeed often the main motivation for the commission of the predicate offence. Laundering of the proceeds of a predicate offence is therefore a logical consequence of many predicate offences, rather than an end in itself.[1597]

The offence of money laundering is thus certainly reprehensible, and the interest of society in the punishment of professional money launderers is not disputed. The degree of seriousness of the crime of money laundering, however, cannot be accepted in an equally undisputed fashion. Both money laundering and terrorist financing are in themselves victimless crimes.[1598] The urgency of their punishment is based solely on the predicate offences in the case of money laundering, and the potential subsequent offences in the case of terrorist financing.

The fact that the seriousness of the crime of money laundering is therefore dependent on the predicate offence generating the laundered funds is now rather at odds with the costly and very far-reaching surveillance measures introduced by the Anti-money laundering Directive.[1599] The Directive's surveillance measures are introduced in order "to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing", as article 1 (1) 4AMLD sets out. The indistinct notion of "suspicious" transactions in the Directive and the extensive catalogue of predicate offences leads, however, to the palpable danger of function creep.[1600] The risk is that the extensive surveillance measures introduced by the Directive, which is ostensibly created to prevent only the two individual crimes of money laundering and terrorist financing, is in fact increasingly or

1596 Hetzer (2008), p. 565.
1597 See Hetzer (2008), p. 565.
1598 See also Lavalle (2000), p. 506; Bentham (1907), p. 204 ff.
1599 Lennon/Walker (2009), p. 41.
1600 Maras (2012), p. 67; Frasher (2016), p. 32.

even primarily used for detecting and investigating the offences in the extensive catalogue of predicate offences.[1601]

It was just argued that the predicate offences of money laundering and the subsequent attacks funded by terrorist financing are much more serious crimes than money laundering and terrorist financing in themselves. Therefore, one would expect that their detection would be a legitimate aim also of the Anti-money laundering Directive. Indeed, the approach to "follow the money", i.e. a paper trail leading the investigators from a suspicious transaction to the predicate offences and their perpetrators, is an intended function of the anti-money laundering legislation.[1602] This is also shown by recital 13 of the proposed fifth Anti-money laundering Directive, which contains the sentence: "In all cases involving money laundering, the associated predicate offences and terrorist financing, information should flow directly and quickly without undue delays."[1603] Indeed, recital 14a 5AMLD goes so far as to state that "The purpose of the FIU is to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity", which shows that the task of the FIU indeed goes far beyond investigating financial crime only.[1604]

However, the ill-defined catalogue of predicate offences creates a difficulty in this regard, which also manifested itself in the Data Retention Directive. In the Data retention Directive, the European lawmaker only referred to "serious crime" in general, leaving the definition of such crimes to the Member States, rather than determining the particular crimes for which law enforcement agencies must be granted access to the data collected by telecommunications providers. The CJEU deplored this lack of proper definition of the applicable crimes and absence of clear purpose limitation, as only the prevention, detection and investigation into the most serious of crimes can justify access to the data retained about individuals by telecommunications providers.[1605]



1601 Article 29 Working Party, Opinion 14/2011, p. 17; Hetzer (2008), p. 565; Hamacher (2006), p. 633 f.

1602 Nestler/Herzog, Geldwäschegesetz, 2. Aufl. 2014, § 261 StGB, Rn. 13; Hetzer (2008), p. 565; Dittrich/Trinkaus (1998), p. 346; Hamacher (2006), p. 633 f. See also the case studies in NCA annual report 2015, p. 27 f.

1603 Recital 13 of the fifth Presidency compromise text 15605/16.

1604 Recital 14a of the fifth Presidency compromise text 15605/16. See also Frasher (2016), p. 32.

1605 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 60. See in this context also Grafenstein (2015), p. 792 f.

When one applies this reasoning to the Anti-money laundering Directive, the very open catalogue of predicate offences raises the same objections. Besides the catalogue of "classical" predicate offences in article 3 (4) (a-e) 4AMLD, article 3 (4) (f) 4AMLD adds a catch-all provision,[1606] according to which all offences punishable beyond a certain threshold in national criminal law must be included as predicate offences.[1607] This particular point creates the exact same situation as was criticized by the Court in *Digital Rights Ireland*: an extensive catalogue of serious crimes, the exact definition of which is left up to the Member States by way of the severity of the penalty accorded to the crime under national criminal law.[1608]

In its *Tele2 Sverige* decision, the CJEU had the opportunity to further develop its reasoning. In that judgment, the CJEU said with great decision that the fight against serious crime as a justification for an extensive retention regime, in this case of traffic and location data, is not sufficient:[1609]

> "Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight."[1610]

The BVerfG goes into more detail when discussing the nature of the serious crime for which retained communications data could be accessed. The Court established that it was insufficient for the lawmaker to define the specific crimes which were to be prevented with the aid of the retained data.[1611] Instead, the lawmaker would have to go beyond defining specific crimes by referring directly to specific legal interests which the retention of data and the access to retained data are to protect.

1606 See Chapter II above.
1607 See also Article 29 Working Party, Opinion 14/2011, p. 15 f.; Dittrich/Trinkaus (1998), p. 346.
1608 Maras (2012), p. 70.
1609 See also United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), p. 6.
1610 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 103. See also Skouris (2016), p. 1364.
1611 BVerfG, 1 BvR 256/08 [2010], paragraph 230.

In addition, the lawmaker must determine a certain level of danger or threat to which those legal interests must be exposed before retained data can be accessed by the authorities.[1612] Based on those considerations, the Court concludes that access to the retained communications data can only be granted to the authorities when positive evidence exist of a concrete danger to public safety, life, limb, or freedom of a person, or the continued existence and security of the Federal Republic or one of its states.[1613] Mere conjecture or general empirical judgments, as the BVerfG clarifies, cannot suffice.[1614]

The same sentiment is expressed by the Council of Europe Commissioner for Human Rights. He shows himself concerned about the blurring of ordinary criminal law and the national security paradigm by states by invoking the fight against terrorism:[1615] "[S]tates can only invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation."[1616]

Applied to the measures taken in the Anti-money laundering Directive, the standard set out therein falls far short of that demanded by the BVerfG and the CJEU. The financial crimes of money laundering and terrorist financing certainly do not pose a sufficient threat to life, limb, or freedom of individuals, public safety, or even the state, to satisfy the BVerfG. Furthermore, the very extensive catalogue of predicate offences also contains a large number of crimes which fall short of the threat level demanded by the Court. This is especially evident when Directive 2016/2258[1617] is considered, which allows access to the information collected and retained by obliged entities by tax authorities.[1618] Tax crimes are purely financial offences, which certainly do not fulfil the standards demanded of serious crime by the BVerfG.



1612 BVerfG, 1 BvR 256/08 [2010], paragraph 230. See also Hamacher (2006), p. 634.
1613 BVerfG, 1 BvR 256/08 [2010], paragraph 231. See also Gurlit (2010), p. 1038; Puschke/Singelnstein (2005), p. 3535; Leutheusser-Schnarrenberger (2014), p. 592; Abate (2011), p. 124.
1614 BVerfG, 1 BvR 256/08 [2010], paragraph 231. See also Gurlit (2010), p. 1038.
1615 See also Maras (2012), p. 68 f.
1616 Korff (2014), p. 108.
1617 Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, OJ L 342, 16.12.2016, p. 1–3.
1618 See additional information on this Directive below.

In practice, few crimes would satisfy these demands. The threshold is thus extraordinarily high. In this context, it is important to point out that the statistics of the German FIU show that the overwhelming majority of money laundering cases merely end with a penalty order.[1619] A penalty order can only be handed down in fast-track procedures in cases of petty offences, and can at worst end in a financial penalty for the offender.[1620] Prison terms can only be imposed in the case of a criminal conviction by an ordinary criminal court. This fact shows that the majority of cases reported in the statistics of the FIU are of very minor importance. They are certainly not examples of serious crimes within the meaning of the term as discussed above.

As has been pointed out above, the German Constitutional Court has stated explicitly that at least in the case of data retention, such minor offences cannot give occasion for the access of retained data by the authorities. The BVerfG stated in its judgment that the retained data can only be accessed by authorities for the prevention, detection, or investigation of a serious crime. Beyond the crime itself being serious, however, the BVerfG also demands that the individual case for which the data is to be accessed is also a serious case of such a serious crime.[1621] Cases of petty crimes resolved in a penalty order very obviously do not meet this demand.

Therefore, in the presence of the fact that the Anti-money laundering Directive is used to aid in the prevention, detection, and investigation into not only the two crimes of money laundering and terrorist financing, but also of an open catalogue of predicate offences for money laundering as well as all offences related to terrorism and tax crimes, it is not clear whether the requirement of a clear purpose limitation of the surveillance measures introduced by the Directive is met. In addition, many of the crimes which are to be prevented, detected, or investigated with the aid of the Anti-money laundering Directive, in particular the crimes of money laundering and terrorist financing themselves, do not pose a threat of a

1619 FIU Jahresbericht 2016, p. 17.
1620 The German provisions concerning penalty orders can be found in §§ 407 ff of the German code of criminal procedure: Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die durch Artikel 15 Absatz 2 des Gesetzes vom 21. November 2016 (BGBl. I S. 2591) geändert worden ist.
1621 BVerfG, 1 BvR 256/08 [2010], paragraph 229. See also Petri (2010b), p. 540 f.

sufficient magnitude to justify the access of the authorities to data retained by the service providers.

The fact that the crimes to which the Directive applies are of varying degrees of seriousness, and generally fall short of the standards urged by the CJEU and the BVerfG has an impact on the balancing act that is proportionality. Particularly serious interferences with the rights of the data subjects can only be accepted where the legislator can show that the measures in question are of particularly high importance. The ill-defined catalogue of offences which are to be combatted by the Anti-money laundering Directive, however, contains many which cannot be regarded as posing a concrete danger to public safety, life, limb, or freedom of a person.[1622] The application of the principle of proportionality therefore limits the legislator in the severity of the measures that can be adopted to combat those crimes.

This concern must be kept in mind by the reader while the measures in question are examined one by one in section (h). The balance between the severity of the measures, the seriousness of the interference they pose, and the objective in the general interest will be revisited in section (i), where the necessity of the measures and the proportionality in *stricto sensu* will be discussed.

## g. Suitability

The assessment of the proportionality of a measure always starts with the question, whether the measure in question is suitable to achieve the aim it pursues. This section seeks to answer this question.



The principle of proportionality can be found in article 5 TEU, along with the principle of conferral and the third element of this triad, the principle of subsidiarity. The principle of proportionality is one of the most important principles in European Union law, because all legislative acts of the Union must adhere to it and can be annulled by the Court when it finds that the legal act falls short of the standards it demands. The importance of the proportionality principle

1622 BVerfG, 1 BvR 256/08 [2010], paragraph 231. See also Gurlit (2010), p. 1038; Bizer (2007b), p. 587.

is also reflected in the amount of judgments in which the Court has had occasion to apply this principle, and in which the Court has judged the legal act at hand to be deficiently proportional, such as, for instance, in the case of the Data retention Directive.

The Court applies a test of three steps in order to determine the proportionality of the disputed legal act. The formula of article 5 is that "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties."[1623] This formula is split into three elements. The first element is *suitability:* The measure must be appropriate to achieve the aim of the Union action. The second element is *necessity*: The measure in question must be necessary in order to achieve the aim pursued by the Union action in question. Finally, a third step is that of *proportionality in stricto sensu*: The measure in question must be reasonable and not excessive. Therefore, only when the Union measure fulfils all three steps of the proportionality test can it be considered as proportionate and as not going beyond what is necessary.[1624]

One fourth element which is explicitly named in the article but only implied in this test is the further condition that the measures must be deployed for a legitimate aim. There is a myriad of legitimate aims already defined in the Treaty, namely the promotion of each area for which the Union has obtained a competence from the Member States, as well as a number of other objectives which the Court has accepted and recognized in its case law.

The legitimate aim has already been discussed in the foregoing section (f). Based on this discussion, the next question is whether the measures set out in the Anti-Money Laundering Directive can fulfil the proportionality standard developed by the CJEU, when the aim of fighting serious crime is contrasted with and weighed against the human rights to data protection and privacy. As has been shown, the Court has consistently applied a three-fold proportionality test, in which the suitability, necessity, and the proportionality *in stricto sensu* are assessed.[1625] As the CJEU stated in its *Digital Rights Ireland* decision, "With regard to judicial review of compliance with those conditions, where interferences with fundamental rights

1623 Article 5 (4), 1st sentence TEU.
1624 Trstenjak/Beysen (2012), p. 271.
1625 CJEU Case 11/70 *Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide* [1970]. Note that the third step is often omitted in cases concerning the free movement rules. For details, see *Shuibhne* in Barnard/Peers (2014), p. 494.

are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference".[1626] The Court then goes on to emphasize that "in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict."[1627] The following section will apply this reasoning of the Court in its judgments on the Data retention Directive to the Anti-money laundering Directive.

The assessment of suitability goes beyond the mere question whether the measure pursues a legitimate aim and is generally capable of achieving it. A further question is whether the measures also pursue this aim coherently and systematically.[1628] In combination, these steps allow the Court a far-reaching analysis and assessment of the content of a measure, as well as its design and implementation. Unfortunately, the Court appears reluctant to use its vast powers in this regard. In its assessment of the suitability of disputed measures, the Court has shown itself consistently cautious and restrained.[1629]

The factor on which the assessment of the suitability of a measure rests is whether the measure is appropriate to achieve the aim for which it was introduced. However, it is extremely difficult to assess the impact of the anti-money laundering measures on the serious crime they were designed to combat, due to the insufficient available information about the shadow economy.[1630] The lack of information on the shadow economy furthermore makes it very difficult to determine whether or not it grew or shrank in the past few years. Even if the estimates on the extent of the shadow economy agree on a certain growth or decline, the reasons for this development can only be guessed at.



1626 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 47. See also Tridimas (1999), p. 76 f.
1627 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 48.
1628 Trstenjak/Beysen (2012), p. 271. See also Manger-Nestler/Noack (2013), p. 505.
1629 Trstenjak/Beysen (2012), p. 271.
1630 See UNODC (no date); Hetzer (2002), p. 413; Collins (2005), p. 84 f.

In principle, however, the additional data which is available to law enforcement through the measures of the Anti-money laundering Directive may be suitable to reach the objectives of the Directive. The CJEU worded this thought in the context of data retention as follows:

> "having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime, and in this respect, they are therefore a valuable tool for criminal investigations."[1631]

Electronic banking is certainly also growing in importance, and the transaction trails could therefore create additional opportunities in the same way as the connection data as discussed in the Data retention Directive.

However, the suitability of the measures as discussed by the Court in its judgment are necessarily solely theoretical. In the following, the development of the anti-money laundering legislation is going to be compared to the tangible results of the legislation. However, it lies in the nature of such an assessment that the full impact of a measure can only be vaguely estimated before it is in fact introduced, and the fourth Anti-money laundering Directive has only entered into force in June 2017. The European anti-money laundering legislation, however, dates back to Council Directive 91/308/EEC, of which Directive 2015/849 is the fourth incarnation. The national FIUs have been recording statistics of obliged parties, reporting, and judicial outcomes since 2003 or earlier.

Reliable numbers exist only concerning the amount of convictions of natural and legal persons of money laundering and terrorist financing. These numbers paint a rather sober picture of the effectiveness of the measures.[1632] For instance, the numbers for Germany may be considered, it being the country with the highest absolute population in the European Union of above 80 million people and home to the large financial centre in Frankfurt am Main. In 2016, the Financial

1631 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 49.
1632 See also Mack (2006), p. 394.

Intelligence Unit of Germany received 40,690 suspicious transactions reports,[1633] the highest number of reports since the earliest statistics in 2003. However, in the same year, only 69 cases of alleged money laundering have ended in a conviction of the defendant.[1634] 284 cases were of sufficiently low importance to qualify for a penalty order.[1635] A penalty order, as has already been mentioned above, is a simplified criminal procedure for petty offences. The overwhelming majority of suspicious transactions reports is dismissed.

Regarding the size of the underground economy, there are no reliable numbers or uniform estimates. As the United Nations office on Drugs and Crime estimates, ca. 2-5% of the global GDP is laundered annually.[1636] The International Monetary Fund estimates that the GDP of the European Union in 2017 lies at nearly USD 17 trillion.[1637] Applying the UNODC estimates to this figure calculates an estimated underground economy of a value of between USD 339 billion and USD 848 billion.[1638]

Thus, it can be safely assumed that the convictions and penalty orders handed down in 2014 only cover a small fraction of the amount of money actually being laundered.[1639] This point is of importance because from a pragmatic or consequentialist perspective,[1640] the immense costs of compliance with the measures of the Anti-money laundering Directive incurred by obliged entities are only justified if the estimated value of the prevented or successfully prosecuted crime is equal to the compliance costs.



1633 FIU Jahresbericht 2016, p. 10. See in this context also Article 29 Working Party, Opinion 14/2011, p. 18 on the number of false positives.
1634 FIU Jahresbericht 2016, p. 17. Indeed, the number of convictions of money laundering in Germany has never exceeded this number, although the number of suspicious transactions reports is rising steadily. Such an observation prompts the Article 29 Working Party to attest "a real risk of confusion" on the part of obliged entities. See Article 29 Working Party, Opinion 14/2011, p. 14.
1635 FIU Jahresbericht 2016, p. 17.
1636 UNODC (no date).
1637 See IMF World Economic Outlook Database, October 2016, accessible at http://www.imf.org/external/pubs/ft/weo/2016/02/weodata/index.aspx last accessed 3 January, 2018. This equals ca. EUR 14.5 trillion.
1638 This amounts to ca. EUR 289-724 billion.
1639 See UNODC (no date).
1640 White (2014), p. 24. See also Solove (2002), p. 1126.

Even less convincing is a survey of the statistics of terrorist financing, concerning which 784 reports have reached the German FIU in 2016.[1641] If any suspicious transactions report has ever lead to any formal court proceeding, the FIU itself is not aware of it.[1642] Indeed, there is so little to report on terrorist financing, that in its annual report 2014, the FIU appears to regard it as a success that one person who was earlier convicted of establishing a terrorist organization was denied an application for a third-party motor insurance for an automobile.[1643] How this denial of that person's application for insurance relates to the fight against terrorist financing is not clear.[1644]

The judgment of the extensive surveillance for such little yield is then also predictably annihilating. The predominant opinion at least among German scholars is that the approach to preventing money laundering and terrorist financing is a failure.[1645] The continuous extension of the application of anti-money laundering measures in Germany over the recent years have increased the number of suspicious transactions reports by several hundred percent since 2003,[1646] reaching over 40 thousand in 2016, each of which represents a serious interference with a data subject's rights to privacy and data protection. The number of convictions of money laundering, however, has only increased marginally. Furthermore, there is no appreciable effect of the anti-money laundering measures on the number of predicate offences. Criminal activity has not been deterred by the anti-money laundering legislation,[1647] and only few suspicious transactions reports lead to an investigation of a predicate offence.[1648]

The same judgment is also found in the international literature. For instance, *Sorel* considers the combat against money laundering "very difficult, impossible even," due to the extremely versatile instruments through which money laundering can be accomplished.[1649]

1641 FIU Jahresbericht 2016, p. 23. This is the highest number of reports of terrorist financing so far. See also Article 29 Working Party, Opinion 14/2011, p. 19.
1642 FIU Jahresbericht 2016, p. 17.
1643 FIU Jahresbericht 2014, p. 39.
1644 See for similar weaknesses in the UK reports NCA annual report 2015, p. 30 f.
1645 Nestler/Herzog, Geldwäschegesetz, 2. Aufl. 2014, § 261 StGB, Rn. 17 ff; Hetzer (2008), p. 565.
1646 FIU Jahresbericht 2016, p. 16.
1647 Nestler/Herzog, Geldwäschegesetz, 2. Aufl. 2014, § 261 StGB, Rn. 15; Hetzer (2008), p. 565.
1648 Nestler/Herzog, Geldwäschegesetz, 2. Aufl. 2014, § 261 StGB, Rn. 15.
1649 Sorel (2003), p. 375. See also Böszörmenyi/Schweighofer (2015), p. 71 f. See also Chapter II above.

Therefore, while the measures of the Anti-money laundering Directive did lead to 69 convictions, and over 280 penalty orders in smaller cases, compared to the overall amount of the money which must be laundered in Germany, the amount of costs incurred by the financial sector, and the scale of surveillance the measures entail, the effect of the anti-money laundering legislation on the underground economy is likely just negligible.[1650] The least one could say is that the effectiveness of the measures cannot be documented.

## h. Necessity and Proportionality in Stricto Sensu

Besides being appropriate to achieve a given aim, the measures must also be necessary. Necessity in this context means that among all the possible appropriate measures, the legislator must choose the measure which impairs the concerned rights and interests in the least possible degree.[1651] This question is also difficult to settle.

It should be noted that the Directive itself anticipates the dispute of its proportionality and states very clearly in recital 64 that the measures established with the Anti-money laundering Directive do not go beyond what is necessary. However, the Directive also ignores the collision of interests between the fight against crime and the protection of privacy and personal data. Instead, it only envisions in recital 2 4AMLD that

> "the objectives of protecting society from crime and protecting the stability and integrity of the Union's financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs."[1652]



The CJEU in its data retention judgement begins the discussion of the necessity of the measures by clarifying that even great importance of the objective of a directive does not sanction extremely far-reaching measures. The Court clarifies that

1650 Sorel (2003), p. 375.
1651 Trstenjak/Beysen (2012), p. 271.
1652 Similarly, the Directive begins with "Having Regard to the opinions of the European Central Bank and of the European Economic and Social Committee", but omits references to the Data Protection Officer or the Article 29 Working Party. See also Zentes/Wybitul (2011), p. 95.

> "it must be held that the fight against serious crime, in particular against organized crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by the Data retention Directive 2006/24 being considered to be necessary for the purpose of that fight."[1653]

Besides suitable and necessary, the measures must finally be proportional in the strict sense, meaning that "there must be an overall reasonable ratio between means and outcome."[1654] This final step is thus a careful balancing of the interests of the state in achieving a certain result, and the interests of the individuals in maintaining their rights as unrestricted as possible.[1655] This balancing of interests is a step of outstanding importance, as it is a safeguard against excessive interferences with human rights through legislative and executive acts. *Exitus acta probat*-approaches are thus from the outset incompatible with EU law.

The application of the third step of the proportionality test would in this case be the question whether the measures of the Anti-money laundering Directive are properly balanced with the two interests of the public[1656] in, on the one hand, the fight against the crimes it covers and, on the other hand, the protection of privacy and personal data.

**i. Concerns**

In order to be able to judge the necessity and reasonableness of the measures of the Anti-money laundering Directive, a number of individual factors that flow into the assessments have been identified, and will be assessed one by one. This section contains seventeen individual sub-sections, which identify and address the most pressing concerns that must be considered in the assessment of the necessity and the proportionality *in stricto sensu* of the measures of the Anti-money laundering Directive.

1653 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 51. See also Skouris (2016), p. 1364; Solove (2007), p. 411.
1654 *Hofmann* in Barnard/Peers (2014), p. 204. See also Solove (2007), p. 411.
1655 See also Waldron (2003), p. 192.
1656 See also Maras (2012), p. 73.

The measures applied by obliged entities have been divided into the four groups identification, monitoring, reporting, and data retention throughout this thesis, and the concerns discussed in this section are also roughly organised along those lines. The first two concerns are major concerns applicable to the anti-money laundering system in general, criticising the mass-surveillance character of the measures. The third concern is closely connected to the identification duties applied by service providers, and the lack of options to use the financial system anonymously. The fourth, fifth, sixth, and seventh concerns are most closely connected to the monitoring duties applied by obliged entities. In those sections, the lack of a definition for the term "suspicious" and the lack of safeguards for sensitive data is criticised , and the implications of the anti-money laundering measures on the presumption of innocence and the service providers' freedom to conduct a business are explored. The eighth, ninth, and tenth concerns are connected to the duty to report suspicious transactions, criticising weaknesses in the reporting obligation, the obligation to comply with requests for information, and the prohibition of disclosure. Closely connected to those three concerns are the following two items: The eleventh point made in this connection is a critique of the lack of transparency, and the twelfth concern is exploring the implications of this lack of transparency and information on the right to an effective remedy. The thirteenth concern begins the discussion of the obligation to retain data with a critique of the lack of meaningful data protection safeguards contained in the Directive. The fourteenth point concerns the retention period, and the fifteenth and sixteenth points concern access to retained data by tax authorities, and the principle of purpose limitation. Finally, the seventeenth point is a look ahead at additional measures to be introduced by the upcoming fifth Anti-money laundering Directive, in particular the proposed databases of bank account holders and virtual currency users.



After walking the reader through these concerns individually, the next section will argue that the balance between the objective in the public interest of combatting serious crime and the rights of privacy and data protection is not even, that the measures restrict the rights to data protection and privacy too much, that the scales are therefore tipped in favour of the rights to privacy and data protection, and that, consequently, the infringements caused by the measures of the Directive are disproportionate.

*(1) Customer Due Diligence Measures as Measures of Mass Surveillance*

The first major concern that can be raised in connection with the measures of the Anti-money laundering Directive is the sheer size of the surveillance it introduces. The Anti-Money Laundering Directive introduces far-reaching untargeted surveillance of all Europeans through several connected measures to facilitate keeping track of financial transactions, known collectively as "know your customer" (KYC) and "customer due diligence" (CDD) measures, pursuant to article 13 4AMLD. Those measures have been discussed in detail in Chapter II above.

In the first place, those measures are carried out to identify the customer and to assess the intended business relationship. Therefore, all customers must be thoroughly identified at the very outset of a business relationship. If the customer is a legal person, the beneficial owner of that legal person must be determined, until one or more natural persons are identified who ultimately stand behind the legal person and benefit from the transactions carried out. Furthermore, the intended business relationship must be analysed before it is entered into (articles 13, 14 4AMLD).

After the customer is thus thoroughly identified, customer due diligence measures must be applied. This mainly concerns transaction monitoring: all transactions carried out during the duration of the business relationship must be analysed and subjected to ongoing monitoring to filter out any transactions which raise a suspicion of money laundering or terrorist financing (article 13 (1) (d) 4AMLD).[1657] If a transaction raises a flag with the institution, the obliged entity must, if possible, refrain from carrying out that transaction, and promptly inform the national FIU of that transaction and forward all relevant information about the customer and the transaction to the FIU (article 33 4AMLD). The customer is not informed of this process (article 39 4AMLD). The FIU then carries out any necessary investigative steps to either reject the case or bring about a case against the customer.

The measures introduced by the Anti-money laundering Directive are so far-reaching that they must be considered to fall into the category mass surveillance. Mass surveillance is the monitoring of the whole or a large part of the population

1657 Article 29 Working Party Opinion 14/2011, p. 7.

without prior suspicion against any particular individual. As *Privacy International* put it,

> "Mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring. It involves a systematic interference with people's right to privacy. Any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance."[1658]

The mass surveillance character of untargeted retention of data in the absence of suspicion has already been acknowledged in the context of the Data retention Directive. The Council of Europe clarifies that

> "[Compulsory suspicionless, untargeted retention of communication records] 'just in case' the data might be useful in some future police or secret service enquiry … ought to be viewed as mass surveillance of citizens without due cause: a fundamental departure from a basic principle of law."[1659]

The particular importance of the protection of the population from excessive surveillance lies in the consideration that an individual can only truly live freely when he or she is not being monitored. If an individual must consider it possible, or even probable, that he is being monitored, and that certain undesirable behaviour is being recorded, processed, and shared, it is likely that he will try to avoid such behaviour that might lead to his being singled out.[1660] But the more surveillance for the more types of undesirable behaviour is being created in public spaces and particularly in (electronic) communications, the more the individual will restrict himself in his behaviour and thus ultimately in the exercise of his freedoms.[1661] That is the reason why excessive surveillance is considered a particularly serious danger for the free and democratic state.[1662]



1658 Privacy international (no date). See also White (2013), p. 23 f.
1659 *Korff and Brown* quoted in Korff (2014), p. 115. See also Bizer (2007b), p. 588.
1660 Martini (2009), p. 841; Maras (2012), p. 74.
1661 See Chapters VI and VII above.
1662 Martini (2009), p. 841; Maras (2012), p. 72. See also BVerfG, 1 BvR 256/08 [2010], paragraph 218.

In *Tele2 Sverige*, the CJEU found very clear words to judge the scale of the surveillance put into place by the data retention regime. It held that "an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight."[1663] In order to assess if this finding of the Court can be applied to the measures of the Anti-money laundering Directive, a look into the scale of surveillance put into place by this Directive is necessary. The scale of the surveillance can be measured by estimating the amount of the population that regularly accesses financial services. In 2011, the European Commission estimated that 7% of the adult inhabitants of the European Union were unbanked, i.e., did not have access to a bank account.[1664] In 2015, the World Bank reported a sharp increase in access to banking services worldwide,[1665] especially in developing countries, but also in Europe.

Indeed, it is impossible to take part in society in most countries in Europe without access to financial services.[1666] In many Member States of the European Union, all inhabitants must absolutely have access to a bank account, as most employers will not pay wages by any other means than by bank transfer, and because it is for the most part impossible to pay taxes, insurances, and rent without a bank account. Therefore, it is not surprising that the number of unbanked persons in Europe is rather small with over 93% of adults in the European Union being holders of a bank account. But they are thereby also subjects to the surveillance introduced by the Anti-Money Laundering Directive.

The current population of the European Union lies at over 510 million.[1667] For simplicity's sake, it could thus be estimated that ca. 500 million individuals in the European Union are subject to surveillance of their financial transactions by

1663 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 103. See also Skouris (2016), p. 1364; Kunnert (2014), p. 776.
1664 European Commission, Commission Staff Working Paper SEC(2011) 907, p. 1. See also Datta (2009), p. 331 f.
1665 World Bank Group, The Global Findex Database 2014, p. 11 ff.
1666 Datta (2009), p. 335. Similarly, the Court held electronic communications to be important in society, cf. CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 56. See also Reddick/Chatfield/Jaramillo (2015), p. 130.
1667 The combined population of the 28 European Member States on January 1st, 2016, as estimated by Eurostat, see http://ec.europa.eu/eurostat/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tps00001&language=en last accessed 3 January, 2018.

the bank at which they hold an account. Those 500 million individuals and the businesses active in the territory of the European Union have carried out ca. 112.1 billion non-cash transactions in 2015,[1668] all of which must have been monitored under the terms of the anti-money laundering regime. The amount of surveillance additionally carried out by other obliged parties cannot be measured. Considering, however, that the group of 'other' obliged parties outnumbers the group of credit- and financial institutions,[1669] the scale of surveillance is extremely high.[1670] It could then be said that the application of the measures of the Anti-money laundering Directive "therefore entails an interference with the fundamental rights of practically the entire European population", as the CJEU said about the Data retention Directive.[1671]

The situation is aggravated by the fact that there are no provisions for exceptions in the Directive. The CJEU has excoriated such a lack of exceptions also in its judgments on the Data retention Directive. It criticised that the Data retention Directive

> "affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exceptions, with the result that it applies even to persons whose communications are subject, according to national law, to the obligations of professional secrecy."[1672]

The Court then continued to criticize that that Directive

1668 ECB (2016), p. 46 (table 6).
1669 FIU Jahresbericht 2014, p. 19.
1670 Böszörmenyi/Schweighofer (2015), p. 72.
1671 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 56. See also Fläming (2007), p. 8; Kunnert (2014), p. 776; Bizer (2007b), p. 588.
1672 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 58; CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 105. See also Hamacher (2006), p. 634.

> "does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relations (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection, or prosecution of serious offences."[1673]

The Anti-money laundering Directive in its turn is equally devoid of exceptions as the Data retention Directive was. In particular, there are no de minimis rules. While money laundering operations normally involve the movement of very large amounts of money, the Directive does not set a threshold of a certain amount, under which the risk of terrorist financing can be regarded as being very low. Indeed, the Directive implicitly rules such de minimis approaches out. For instance, article 11 4AMLD provides for customer due diligence measures to be applied by obliged parties other than credit- or financial institutions if certain thresholds are met. The thresholds can, however, also be met cumulatively through "several operations which appear to be linked". What precisely is meant by 'linked' is not clear. It can be difficult for an obliged entity to establish such links and chains of transactions. The danger they face is that the first link in a beginning chain of transactions is not observed properly, leading to an increased difficulty in linking a second transaction to the first. Therefore, to make absolutely sure that those obliged entities do not miss the fact that transactions are linked, they would have to apply consumer due diligence measures at a much lower threshold already, thereby cancelling out the protection of the thresholds in that article altogether. Similarly, the reporting obligations spelled out in article 33 (1) (a) 4AMLD explicitly deny any thresholds, compelling obliged entities to assist the FIU by:

> "informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases".

1673 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 59; CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 106.

In addition to a lack of a de minimis rule, there are also no material exceptions, such as specific categories of transactions which can be exempted from the ongoing monitoring obligations of obliged entities, such as, for example, small amounts paid at grocery stores.[1674] Indeed, such exceptions cannot be effectively granted, as the transactions must be ran through the monitoring system in order to determine whether or not they would fall under such a low risk category. An interference with the customer's rights to privacy and data protection can therefore never be avoided under the existing system.

The Directive does allow for very narrow exceptions to the rigorous customer due diligence system. There are groups of transactions in which 'simplified customer due diligence' measures can be applied (articles 15-17 4AMLD). Which parts of the process are simplified exactly, and how, is however not expressly explained by those articles, but article 15 (3) 4AMLD stipulates that "Member States shall ensure that obliged entities carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions",[1675] which in effect negates all meaningful limitations to the scale of surveillance.

Besides the material exceptions, personal exceptions are also lacking from the text of the Directive. There are some parties which are exempted from the strict consumer due diligence regime under national law and who receive privileged treatment by simplified consumer due diligence measures, but those apply to only a very small share of transactions. For instance, German national law collects some examples in § 5 of the Anti-money laundering Law (*Geldwäschegesetz*, GwG).[1676] Privileged parties include, for instance, other obliged parties, publicly traded company quoted on a European stock exchange, and public authorities. There are no exceptions for ordinary individuals who are unlikely to ever become involved in money laundering investigations.

Finally, it should not be forgotten that large areas, such as for instance cash transactions, are hardly monitored. Cash transactions are only covered by the Anti-money laundering Directive if they reach the amount of EUR 10 000. A similar

1674 See also Rossum et al. (1995), p. 41 ff.
1675 See in this context also Maras (2012), p. 69.
1676 Geldwäschegesetz vom 13. August 2008 (BGBl. I S. 1690), das zuletzt durch Artikel 7 des Gesetzes vom 11. April 2016 (BGBl. I S. 720) geändert worden ist.

gap is the coverage of virtual currencies, which also elude regulation to a large extent. The measures introduced by the Anti-money laundering Directive might thus introduce but a minor inconvenience in international money laundering and terrorist financing.[1677]

The comprehensive scope of the Directive and the character of mass surveillance that the measures contained therein assume, is the first concern regarding the proportionality of these measures.[1678] The text of the Directive is entirely devoid of meaningful personal or material exceptions. The remarks made by the CJEU in its data retention judgments are equally valid for the Anti-money laundering Directive. This lack of exceptions means that the terms of the Directive "applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[1679] The importance of this point can hardly be underestimated. Based on this comprehensive scope of the Directive alone, it may already be said that the measures contained in the Directive go beyond what is necessary.[1680]

***(2) No Accommodation for Professional Secrecy***

Closely connected to the foregoing is a second concern, which is the lack of exceptions for persons whose connection with their clients are covered by guarantees of professional secrecy under national law.[1681] In its *Digital Rights Ireland* judgment, the CJEU criticised that the Data retention Directive "does not provide for any exceptions, with the result that it applies even to persons whose communications are subject, according to national law, to the obligations of professional secrecy."[1682]

1677 See, however, European Economic and Social Committee 13666/16, p. 7, where the EESC states that it "agrees in principle with the measures proposed in the 5AMLD and believes that they may prove useful in helping to put an end to terrorism and money laundering." No other agency expressed itself quite so hopeful.

1678 Milaj/Kaiser (2017), p. 121.

1679 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 58; CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 105. See also Hamacher (2006), p. 634.

1680 See also United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), p. 19 f.

1681 See in this context also CJEU Case C-145/83, *Adams v. Commission* [1985], paragraph 34.

1682 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 58; CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 105. See also Hamacher (2006), p. 634; Gärtner/Kipker (2015), p. 597 f.; Bergemann (2007), p. 584; Bizer (2007b), p. 589.

It should be pointed out in that regard, that the Anti-money laundering Directive does create one very limited exception in article 34 4AMLD. That article provides that auditors, external accountants, tax advisors, notaries and other independent legal professionals, who are obliged parties according to article 2 (1) point (3) (a) and (b) 4AMLD, can be exempted from reporting to the FIU, and report suspicious activity instead to the self-regulatory body of their profession, such as the bar association.[1683] However, that body must then "forward the information to the FIU promptly and unfiltered" (article 34 (1) second sub-paragraph 4AMLD), rendering the exception largely meaningless. Indeed, instead of any form of protection this provision only creates additional inefficiency and paperwork, not to mention an additional risk where the financial data relates to sensitive data.[1684]

Meaningful protection of the professional secrecy of those obliged entities is only provided by the second paragraph of article 34 4AMLD:

> "Member States shall not apply the obligations laid down in Article 33(1)[1685] to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings."

A similar exemption can be found in article 14 (4) 4AMLD concerning the identification of clients. This exception is in principle in line with the case law of the CJEU:

> "Lawyers would be unable to carry out satisfactorily their task of advising, defending and representing their clients, who would in consequence be deprived of the rights conferred on them by Article 6 of the ECHR,

1683 See CJEU Case C-305/05, *Ordre des barreaux francophones et germanophone and Others v Conseil des ministers* [2007]. See also Tracfin annual report 2015, p. 23.
1684 See also Chapters II and V above, and the fifth concern discussed below.
1685 The obligation of article 33 (1) 4AMLD is the obligation to report suspicious transactions and to comply with requests for information made by the FIU. Footnote added by the author.

> if lawyers were obliged, in the context of judicial proceedings or the preparation for such proceedings, to cooperate with the authorities by passing them information obtained in the course of related legal consultations."[1686]

Therefore, this narrowly defined number of obliged entities are only exempted from reporting suspicious activity of their clients when such reporting would manifestly violate the right to a fair trial of article 47 of the Charter. However, the limits of the provision in article 34 (2) 4AMLD are not defined with much clarity. For instance, where a lawyer is representing a client in judicial proceedings, the lawyer needs not report information concerning that client and that proceeding, even where information was obtained before the proceeding. However, if information is obtained before the proceedings, the lawyer cannot be certain ex ante that this information will be covered by the exception in article 34 (2) 4AMLD. How this provision will be applied in such circumstances is not yet certain. In addition, if any other obliged party is involved in the transaction, that obliged party is of course not exempted from the obligation to report.

Therefore, the measures of the Anti-money laundering Directive also create a danger to the right to a fair trial. While the exemption in article 34 (2) 4AMLD is decidedly a step forward compared to the complete absence of protection in the Data retention Directive, the exemption is still extremely narrow. This is raising another concern against the Anti-money laundering Directive, as in principle, the right to a fair trial in article 47 of the Charter should be the norm, exceptions to which should be interpreted narrowly. The Directive turns this situation around: The absence of protection is the norm, with a narrow window for the protection of article 47 of the Charter. This approach is another grave concern that should be considered in the proportionality assessment.

***(3) Erosion of Anonymity***

A third concern that should be addressed in this context is that the options for anonymous transfer of funds are now extremely limited. Before the advent of the massive use of online banking, anonymity was to a large extent the standard for

1686 CJEU Case C-305/05, *Ordre des barreaux francophones et germanophone and Others v Conseil des ministers* [2007], paragraph 32.

financial transactions.[1687] The great majority of day-to-day transactions were made in cash, and only the larger transactions as well as the transactions where the parties were located at a great distance from one another were carried out through bank transfers and cheques. The anonymity of transactions resulted from the fact that cash was used in such a great number of transactions, and cash is by definition anonymous.[1688]

This anonymity was slowly eroded over the last decades by the ubiquity of electronic transactions, which allow for transactions to be tied directly to an identity and which also record a host of other data, such as the time and amount of the transaction, as well as the recipient. Anonymity, however, is particularly attractive in financial transactions, as financial data is so very vulnerable to theft. The more electronic transactions are used, the more points of attack are created for the theft of this data. Financial data is data particularly often compromised, often without the immediate knowledge of the individual or the financial institution. A massive amount of credit card information can be bought on the dark web, for instance, causing serious economic damage to the financial sector. Security is increased by encryption and a number of other security measures, but the large amount of transactions also mean that a large number of parties have access to one's financial data, such as financial services providers, but also recipients of payments. Security and encryption cannot be ensured for all of those parties, especially in databases of small economic players.

Anonymous means of transaction have the great advantage of not being connected to one another, and therefore a greater number of anonymous transactions does not increase the vulnerability of the user's data.[1689] Virtual currencies for instance, though not anonymous, could offer a great advantage in this regard by offering secure transactions which do not directly reveal the parties' identities to one another, thereby ensuring that the security of the data of the users of those systems are not only dependent on the diligence of the other party to the transaction. This mechanism is a potentially great advantage to users wishing to increase the level of protection of their identity and privacy.[1690]



1687 See for a more detailed discussion of anonymity Chapter VII above.
1688 See for more information on the anonymity of cash Chapter III above.
1689 See also Nicoll/Prins (2003), p. 289. See also Chapter VII.
1690 This is explained in detail in Chapter VII. See however also section (j) of this chapter below.

Such a protection is not an option when entities compliant with their obligations under the Directive are involved in the transaction. The Anti-money laundering Directive very decidedly creates safeguards against anonymity in financial transactions. Article 10 (1) 4AMLD provides that

> "Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks. Member States shall, in any event, require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way."

This provision leaves in principle only cash as an anonymous available tool for financial transactions. Cash, however, is not of practical use in many transactions, particularly in e-commerce. Furthermore, while many European Member States are slowly progressing towards a cashless economy, the options for the use of cash are further limited.

However, the inexistent options for anonymity in financial transactions are also in conflict with data protection legislation. The principle of data minimization would demand at least some options for anonymity to remain available.[1691] According to article 5 (1) (c) of the GDPR, the collected personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The same principle is found in article 4 (c) of the Police and Criminal Justice Authorities Directive, which stipulates that personal data collected and processed under the terms of the Directive must be "adequate, relevant and not excessive in relation to the purposes for which they are processed". The principle of data minimization therefore basically demands that only as much data as is necessary for a given purpose should be processed. This concerns in particular small transactions of low risk, such as purchases in a grocery store.[1692] It is possible for the buyer to purchase goods anonymously using cash, but when using a bank card to instantly transfer the purchase price electronically, this triggers a chain of

1691 This notion has been discussed also in Chapter VII section (c) above. See also Schantz (2016), p. 1841 f.; Katzenbeisser (2016), p. 99 f.
1692 See also Rossum et al. (1995), p. 41 ff.

serious interferences with his privacy. There appears to be no satisfactory logical explanation for this discrepancy.

This ubiquity of identification in financial transactions is a further concern in this context that should flow into the proportionality assessment of the terms of the Anti-money laundering Directive.

***(4) Lack of Transparency concerning Suspicious Transactions***

A fourth concern is the unclear definition of the term 'suspicion' that is so central to the construction of the Directive. The ill-defined term 'suspicious transaction' is a major weakness of the construction of the Directive, raising questions as to the foreseeability of measures triggered due to 'suspicions'.

The notion of a suspicious transaction is elusive. The Directive contains no definition of the term 'suspicious', nor does it provide for any indications about how the term is to be applied by obliged entities. Obliged entities are, in fact, completely left to their own devices by the text of the Directive. A similar problem is posed by the long blacklist of persons and companies that are considered to have a connection to terrorist groups[1693] and the lists of politically exposed persons. Those lists are subject to constant change, but all transactions must be checked against those lists in order to make sure that none of the obliged entity's own customers becomes included in such a list, or that the counterparty to a transaction is not on a list.[1694] Several commercial solutions are available to aid companies in fulfilling this obligation, but the quality of those solutions is not uniform.[1695] In fact, there are as yet no standards which such a software would have to comply with, which would further such uniformity.[1696] Naturally, the authors of such software consider the output the software provides as non-binding and reject all liability, despite the high costs of these systems.[1697]



1693 See CJEU Case C–402/05 P and C–415/05, *P. Kadi and Al Barakaat International Foundation v. Council and Commission* [2008]; CJEU Case T-47/03, Jose Maria Sison v Council of the European Union [2007]; CJEU Case T-341/07, *Jose Maria Sison v Council of the European Union* [2011]. See also Ryder (2007), p. 830 f.; Arnauld (2013), p. 236 ff.

1694 See also De Goede (2011), p. 506 f.

1695 Hohenhaus (2016), p. 1047. See also Ryder (2007), p. 830 f.

1696 Hohenhaus (2016), p. 1047.

1697 Hohenhaus (2016), p. 1047.

Naturally, the lack of a definition of what is considered suspicious activity is also a disadvantage for customers of an obliged entity. The customer can only have a vague notion of what kind of behaviour may be considered suspicious by his service provider, which makes it to some extent unforeseeable for the customer under what circumstances his data might be transmitted in a suspicious transactions report.[1698] This lack of foreseeability is incompatible with the principle of lawfulness, fairness, and transparency, mentioned also in article 5 (1) (a) of the GDPR, which sets out that all personal data must be "processed lawfully, fairly, and in a transparent manner in relation to the data subject".[1699]

In this context, it must be pointed out that article 4 (a) of the Police and Criminal Justice Authorities Directive only stipulates that personal data collected and processed under the terms of the Directive must be "processed lawfully and fairly". The Directive thus does not mention transparency. However, transparency of processing in this regard is essential for the accountability of law enforcement activity.[1700] A lack of accountability in this regard would be incompatible with the right to a fair trial under article 47 of the Charter. The omission of the term 'transparency' in the Police and Criminal Justice Authorities Directive does not excuse law enforcement agencies from observing the level of transparency demanded of the authorities under the right to a fair trial.

At this point, the definition of a suspicious transaction is largely left up to algorithms by which transactions are monitored. Accountability is of such high importance in this regard because the algorithms by which suspicious transactions are identified and flagged are not laid open to the public or subject to oversight or review. Indeed, they are often considered a business secret.[1701] It is therefore also not known what kind of information is taken into account in the monitoring, and whether ethnic profiling and other illegitimate practices are taking place.[1702]

1698 See also Tolani (2007), p. 279 f.
1699 See for a more detailed discussion of this principle Chapter V section (d) above.
1700 Raab (2014), p. 56.
1701 See Kaetzler (2008), p. 175; Zentes/Wybitul (2011), p. 93.
1702 Wensink et al. (2017), p. 151. See also Article 29 Working Party, Opinion 14/2011, p. 19; Lennon/Walker (2009), p. 41; Maras (2012), p. 73; Favarel-Garrigues/Godefroy/Lascoumes (2011), p. 183 f.

This lack of transparency concerning such central terms in the Directive is another factor that should be taken into account during the assessment of the proportionality of the measures of the Anti-money laundering Directive.

*(5) No Safeguards for Sensitive Data*

A major concern that must be addressed is the complete lack of safeguards for special categories of data.[1703] In principle, processing of sensitive information is prohibited.[1704] According to article 9 (1) GDPR,

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

This prohibition, however, comes with a rather long list of exceptions, among which is article 9 (2) (g) GDPR, which allows processing where

> "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"

The lawmaker is classifying the fight against money laundering and terrorist financing as a substantial public interest, and processing of the sensitive data is occurring on the basis of the Directive. However, the Directive does not meet the other conditions mentioned in article 9 (2) (g) GDPR, under which the exception can apply. It is the purpose of this chapter to argue that the measures are not proportionate to the aim pursued. While the evaluation of the proportionality of the measures will take place at the end of this section, it can already be said at this point that the Anti-money laundering Directive is devoid of "suitable and specific measures to safeguard the fundamental rights and the interests of the data

1703 See also Frasher (2016), p. 32.
1704 See Chapter V above.

subject". In fact, the Directive entirely devoid of measures to specifically safeguard the sensitive data of the data subject.

The Police and Criminal Justice Authorities Directive is somewhat stricter with sensitive data than the GDPR; it does not provide for nearly as many exceptions. Article 10 of the Directive reads,

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:
>
> (a) where authorised by Union or Member State law;
> (b) to protect the vital interests of the data subject or of another natural person; or
> (c) where such processing relates to data which are manifestly made public by the data subject."

This provision of the Police and Criminal Justice Authorities Directive, when applied to the measures of the Anti-money laundering Directive, shows the rather serious shortcoming of the latter. Sensitive data may only be processed if the processing is (1) "strictly necessary", (2) "subject to appropriate safeguards for the rights and freedoms of the data subject" and (3) "where authorised by Union or Member State law", or "to protect the vital interests of the data subject or of another natural person", or "where such processing relates to data which are manifestly made public by the data subject." As has been pointed out above, this thesis argues that the processing of data under the Anti-money laundering Directive exceeds the limits of the principle of proportionality. The first condition is therefore already not met. The second condition that appropriate safeguards must be introduced is also not met, as the Anti-money laundering Directive is entirely devoid of any safeguards for sensitive data. Finally, the vital interests of the data subject are not involved in the processing of his or her data under the Anti-money laundering Directive, nor did the data subject make this data public. Point (a) concerning the authorisation of the processing is a point which could be argued: the Anti-money

laundering Directive certainly authorises the processing of personal data. It does not, however, explicitly authorise the processing of sensitive categories of personal data. A general authorisation to process personal data is, however, insufficient for the processing of sensitive categories of data. The conditions for processing sensitive data in article 10 of the Police and Criminal Justice Authorities Directive are therefore not met.

Most of the sensitive data that processed in connection with the anti-money laundering measures is processed inadvertently. However, that sensitive data is processed inadvertently, as a by-catch as it were, does not excuse the lack of safeguards to flank this processing. Indeed, this omission should have been recognised and foreseen by the lawmaker, and addressed by introducing specific safeguards.[1705]

In a recent opinion, the CJEU has had occasion to emphasise the importance of the protection of sensitive categories of data.[1706] In its opinion on the PNR agreement between Canada and the European Union, the Court has emphasised the importance of the protection of sensitive data:

> "As regards the transfer of sensitive data within the meaning of Article 2(e) of the envisaged agreement, that provision defines such data as any information that reveals 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership', or concerning 'a person's health or sex life'. Although none of the 19 headings set out in Annex to that agreement expressly refers to data of that nature, as, inter alia, the Commission confirmed in its answer to the questions posed by the Court, such information could nevertheless fall within the scope of heading 17.[1707] Furthermore, the fact that Articles 8 and 16 of the envisaged agreement lay down specific rules relating to the use and retention of sensitive data necessarily implies that the parties to that agreement have accepted that such data may be transferred to Canada.

1705 See in this context also Weichert (2015), p. 18; Bergemann (2007), p. 583 f.; Starosta (2010), p. 238.
1706 See Chapter VIII above.
1707 Heading 17 of the proposed agreement contained a free space for "general remarks". Footnote added by the author.

> In this connection, it must be pointed out that any measure based on the premiss that one or more of the characteristics set out in Article 2(e) of the envisaged agreement may be relevant, in itself or in themselves and regardless of the individual conduct of the traveller concerned, having regard to the purpose for which PNR data is to be processed, namely combating terrorism and serious transnational crime, would infringe the rights guaranteed in Articles 7 and 8 of the Charter, read in conjunction with Article 21 thereof. Having regard to the risk of data being processed contrary to Article 21 of the Charter,[1708] a transfer of sensitive data to Canada requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime. In this instance, however, there is no such justification."[1709]

Naturally, the circumstances of the PNR agreement and the Anti-money laundering Directive are rather different. However, the insights of the Court are still very valuable when applied to the Directive. In particular, the CJEU's opinion on the PNR agreement shows that the Court is placing much emphasis on the protection of sensitive data. The Court is emphasising the risk of discrimination inherent in the processing of passenger name records, due to the problematic nature of the selectors which may be applied to this data.[1710] This is a concern which can easily be transferred to financial data processed under the Anti-money laundering Directive: The same discriminatory selectors which could be applied to PNR data may also be applied to financial data. In this way, the protection of sensitive data is closely connected to the unclear notion of suspicious transactions as noted above.[1711]

The purpose of the PNR agreement was to transfer data out of the European Union, which increases the risk that insufficient safeguards are applied to the use of sensitive data.[1712] The subject matter of the Anti-money laundering Directive is different in this regard, as the transfer of data to third countries is not a primary

1708 Article 21 of the Charter of Fundamental Rights of the European Union is the Right to Non-discrimination. Footnote added by the author.
1709 CJEU Opinion 1/15 *PNR* [2017], paragraphs 164-165.
1710 Frowd (2012), p. 409 f. See also González/Bessa (2012), p. 295 f.
1711 See also the fourth concern discussed in this Chapter above.
1712 See in this context also Polčák (2014), p. 285 ff. on the issue of jurisdiction in data protection.

objective of the Directive. However, data processed under the terms of the Directive is often transferred within the European Union and also moved to third countries.[1713] The proper protection of sensitive data would demand, however, that the Directive contains special provisions concerning such data, exempting them from being processed unless there are specific and potent reasons for doing so.

In its opinion on the PNR agreement, the Court declared the rules contained in the agreement incompatible with the rights to privacy and data protection in connection with the right to non-discrimination.[1714] It is possible, even likely, therefore, that the Court will decide in the same fashion when confronted with the utter lack of safeguards in the Anti-money laundering Directive. If the Anti-money laundering Directive were ever challenged before the CJEU, the Court could deem the Directive incompatible with the rights to privacy and data protection on the basis of the utter lack of safeguards for sensitive data alone. Therefore, this is a very important factor to count into the proportionality assessment.

***(6) Lack of Respect for the Presumption of Innocence***

A sixth point that should be taken into account in the assessment of the proportionality of the anti-money laundering measures is the connection between the surveillance they introduce and the presumption of innocence. The principle of the presumption of innocence is one of the most fundamental and most indispensable general legal principles recognised under Union law. This principle can be found in all modern declarations of human rights, prominently in article 6 (2) of the ECHR, which reads "Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law." The same principle can be found in article 48 (1) of the Charter of Fundamental Rights of the European Union, in almost the same words: "Everyone who has been charged shall be presumed innocent until proved guilty according to law." It is also a part of the principles which make up the concept of rule of law, and is understood to apply at all stages of the criminal process.[1715]



1713 FIU Jahresbericht 2016, p. 21. Note that the FIU here reports that it expects a sharp increase in the exchange of information among FIUs as soon as the fourth Anti-money laundering Directive entered into force. See in this context also Moerel (2011), p. 106 ff. on the SWIFT system, which facilitates the exchange of financial data to facilitate carrying out transactions.

1714 CJEU Opinion 1/15 *PNR* [2017], paragraph 232. See in this context also Bou-Habib (2008), p. 161.

1715 Milaj/Mifsud Bonnici (2014), p. 421. See also Galetta (2013), p. 2; Hadjimatheou (2014), p. 194.

There is an ongoing debate on whether the principle of the presumption of innocence extends to the investigatory stages before the initiation of a formal legal process against an individual.[1716] However, while arguably this extension was not originally intended by the lawmaker, the principle has begun to grow beyond the confines of a criminal process. Indeed, it is difficult to imagine a situation in which the presumption of the innocence of an alleged offender is denied him before the process, just to be re-established at the commencement of the proceeding. In this way, the presumption of innocence has to some extent grown into a principle of civility, which "imposes a duty on all to presume, until the contrary has been proven, that people are acting in accordance with their important social obligations."[1717] The application of preventive measures of mass surveillance against the possible commission of certain crimes, however, naturally begs the question whether the subjects of such surveillance are thus indeed considered innocent and to be acting in accordance with their obligations, or if they are not already universally suspected.[1718]

This question is very relevant when the provisions of the Anti-money laundering Directive are considered.[1719] The weakness in the application of this principle lies in the fact that no customer of an obliged entity can escape the far-reaching surveillance measures applied to him.[1720] The surveillance is put into place as a guard against the possibility that the customer uses the services for the purposes of money laundering or terrorist financing, independent of evidence relating to the individual customer. The customer is thus from the outset suspected of potentially committing a crime.

When persons not suspected of having committed any crimes come into contact with law enforcement, it is usually as victim or witness, or otherwise related to a certain incident.[1721] The data of such persons is usually handled differently by law enforcement agencies than data related to a suspect (article 6 of the Police and Criminal Justice Authorities Directive). Data of persons falling outside of any of such categories should in principle not be processed by the authorities. As the Article 29 Working Party points out,

1716 Hadjimatheou (2014), p. 194.
1717 Hadjimatheou (2014), p. 195.
1718 Milaj/Mifsud Bonnici (2014), p. 421 f.; Hirsch (2008b), p. 89.
1719 See also Arzt (1990), p. 5.
1720 Murck (2013), p. 96. See also Korff (2014), p. 29 f.; Marx (2003), p. 369 f.
1721 Boehm/De Hert (2012), p. 2.

> "Processing of data of persons who are not suspected of having committed any crime (other than victims, witnesses, informants and associates) shall be strictly distinguished from data of persons related to a specific crime and 'should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose.'"[1722]

This is not the case in the Anti-money laundering Directive, which places every customer of the financial sector under the same surveillance regime.

> "Furthermore, such processing should (in the view of the data protection authorities) 'be restricted to a limited period and the further use of these data for other purposes should be prohibited.' A specific protection of 'non-suspects' is particularly required when the processing is not done in a specific criminal investigation or prosecution."[1723]

This is the case in the context of most of the processing carried out under the Anti-money laundering Directive. The monitoring of transactions concerns data subjects, the overwhelming majority of whom are not suspected, and never will be suspected, of money laundering. Yet, they are evidently treated as though they were.[1724]

This approach favoured by the Anti-money laundering Directive can be observed also in other pieces of legislation; it is indeed a predominant approach in modern policing.[1725] The Council of Europe Commissioner for Human Rights has shown himself concerned that "the emphasis is increasingly on intelligence and prevention rather than *ex post facto* law enforcement."[1726] This way, the strategy formerly applied mostly by intelligence services and national security agencies is now coming to be applied in other areas of policing and law enforcement,[1727] including anti-money laundering. The difficulty lies in the fact that many of the anti-money laundering measures, particularly the identification, monitoring, and data retention duties,



1722 Article 29 Working Party Opinion 3/2015, p. 7.
1723 Article 29 Working Party Opinion 3/2015, p. 7.
1724 Galetta (2013), p. 5 f.
1725 See also Hirsch (2008a), p. 25.
1726 Korff (2014), p. 29 f. See also Custers/Vergouw (2015), p. 524 f.
1727 Korff (2014), p. 29 f.

are applied to all customers of a financial services provider pre-emptively ex ante, in the absence of any reasonable grounds for suspicion, rather than ex post against suspects of crime identified by law enforcement agencies.[1728]

It is the obligation of the competent authorities to prove beyond reasonable doubt the guilt of a person, rather than that it were the individual's obligation to prove his innocence.[1729] It is, of course, impossible to prove a negative: The customer can never prove himself innocent of the crime of money laundering.[1730] He or she may show that he or she has never been convicted of money laundering, or even that none of his or her other transactions have previously led to investigations. This is, however, made difficult for the customer for the fact that he or she is not notified of suspicious transaction reports, as will be seen in the following sections.[1731] But the suspicion against the customer as a possible money launderer does not only concern the past. Although a customer may have never given occasion to any financial services providers he or she has been involved with to report any of his or her transactions, the future is by definition uncertain. The fact that a customer is not involved, or at least has not been caught in such involvement, in money laundering operations in the past does not allow any conclusions to be drawn concerning his or her future lack of involvement in a money laundering scheme.[1732] This, at least, is the assumption under which the Anti-money laundering Directive operates.

In the words of the CJEU in its data retention judgement, the application of the Directive

> "affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[1733]

1728 See also Maras (2012), p. 68.
1729 See also Gerstein (1984a), p. 247 f.; Wasserstrom (1984), p. 322 f. See in this context also Singelnstein/Derin (2017), p. 2648.
1730 See in this context also Gerstein (1984a), p. 247 f.
1731 This is the subject of the tenth concern discussed below.
1732 See also Hamacher (2006), p. 634.
1733 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 58.

The same is true for the Anti-money laundering Directive, which affects in the majority of cases the respectable citizens against whom no allegations have ever been made. The majority of them will also in the future never give occasion for investigations This sixth concern is an important point to take into account during the proportionality assessment.

***(7) Interference with the Freedom to Conduct a Business***

The seventh point that should be mentioned is relatively minor compared to the other concerns listed in this section, but nonetheless it adds an important additional angle to the discussion. It has been mentioned several times already that the costs of compliance with the measures prescribed by the Directive are very high. Particularly the continual monitoring of transactions can be a serious drain of resources for an obliged entity.[1734] The seventh concern to be addressed in this regard applies to the implications of the monitoring and reporting duties on the freedom to conduct a business of the obliged entity (article 16 of the Charter).

A similar system of monitoring has already been assessed by the Court in a different context.[1735] In its 2010 decision in *SABAM*, the CJEU decided that a system in which internet service providers would need to actively monitor customer data in order to be sure that their services are not used for intellectual property rights infringements is incompatible with European Law.

> "In that regard, the Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as a hosting service provider, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual-property rights. Furthermore, such a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly".[1736]

Therefore, while all businesses must comply with a number of legal obligations, there is a limit to the obligations which can reasonably be placed on the service

1734 See in this context also Guggenberger (2017), p. 2578 f.
1735 See also Chapter VIII above.
1736 CJEU Case C-360/10, *SABAM* [2010], paragraph 34.

provider. The limit defined by the CJEU in SABAM was that measures to be taken by businesses must be fair and proportionate, and should not burden businesses with excessive costs.[1737]

Naturally, this remark of the Court cannot necessarily be applied directly to the Anti-money laundering Directive, for the situation of internet services providers and financial services providers is very different. Hosting services providers are explicitly protected by article 15 of the E-commerce Directive,[1738] which prohibits just such an obligation to monitor traffic.[1739] This obligation is further supported by article 3 of the Enforcement Directive,[1740] which, as was also mentioned by the Court above, demands that measures which are taken by service providers to guard against intellectual property infringements must be proportionate and not too expensive for the service provider.

There is no such provision protecting the financial services industry, although the situations are rather similar. Both cases, internet services providers and financial services providers, concern businesses whose services should not be abused for illegitimate activity. While the two crimes are of a widely different nature, it is still striking that internet services providers are to a large extent protected against disproportionate obligations to monitor, while financial services providers are burdened in such an excessive way by anti-money laundering measures. It is not at all certain how the Court would regard the obligations burdening financial services providers. If these measures were ever challenged based on the interference with the freedom to conduct a business, but it is certainly possible that the Court would consider these obligations to be a disproportionate interference with this freedom.

This is a concern which is in principle unrelated to the rights to privacy and data protection. However, it should be kept in mind that although so many concerns are listed in this section which are connected to the rights to privacy and data protection, the Directive may also be challenged based on the economic freedoms

1737 CJEU Case C-360/10, *SABAM* [2010], paragraph 34.
1738 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16. See also Guggenberger (2017), p. 2581 f.
1739 Cunha/Marin/Sartor (2012), p. 53 ff.
1740 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance), OJ L 157, 30.4.2004, p. 45–86.

of obliged entities. Indeed, viewed from this standpoint, the outcome of a proportionality assessment would likely also be negative.

***(8) Excessively Wide Reporting Obligations***

The eighth point that should be made in this context will begin the discussion of concerns connected to the obligation to report suspicious transactions. Along with the obligation to monitor all transactions carried out over their systems, the obligation to report suspicious transactions is a particularly explosive liability on the side of obliged entities. This obligation falls into three related subjects: In the first place, all suspicious activity must be reported to the Financial Intelligence Unit. In the second place, the obliged entity must comply with requests for information, which will be discussed in the ninth place below, and thirdly, no information about such a report may be relayed to the data subject, which is the subject of the tenth concern below.

It has already been explained that all reports of suspicious activity detected by obliged entities are relayed to the local FIU. Financial Intelligence Units are established in each Member State in accordance with article 32 4AMLD. In its third paragraph, this article provides that,

> "Each FIU shall be operationally independent and autonomous, which means that the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information."

The information in question does not only relate to the suspicious transactions reports collected from obliged parties, but can also relate to information received from other sources. Paragraph (4) of the same article stipulates that

> "Member States shall ensure that their FIUs have access, directly or indirectly, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly. FIUs shall be able to respond to requests for information by competent authorities in their respective Member States when such requests for information are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing. The decision on

> conducting the analysis or dissemination of information shall remain with the FIU."

These "maximum powers of access to national databases" have been criticized especially in the discussions of the previous third Anti-money laundering Directive, as that previous Directive was marked by a complete absence of data protection provisions.[1741] While the fourth Directive does contain a provision addressing data protection, it will be seen in point thirteen below that the data protection clause cannot be considered to contain any meaningful safeguards.[1742]

The powers of the FIU are thus very broad and hardly accompanied by safeguards and limitations. The fourth and fifth Anti-money laundering Directives each contain a specific provision which stipulates that the FIU may refuse to share information upon request if "disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested", but such a refusal can only be applied "in exceptional circumstances" (article 32 (5) 4AMLD). There is no corresponding provision allowing other public entities or obliged entities to refuse requests for information from the FIU, not even in exceptional circumstances.

All obliged entities are then obliged to report all suspicious activity to the local FIU. The transmission of suspicious transaction reports is regulated in article 33 (1) (a) 4AMLD, which places the duty on all obliged entities to collaborate by notifying the FIU

> "on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases".[1743]

This widely-worded obligation to report has resulted in a veritable flood of reports constantly forwarded to the FIUs. The excessive amount of paperwork thus

1741 Mitsilegas/Gilmore, (2007) p. 127. See in this context also Boehm (2012), p. 341 f. See also the thirteenth concern discussed in this chapter below.
1742 See also FIU Jahresbericht 2016, p. 20 f. on information exchange.
1743 See also Article 29 Working Party, Opinion 14/2011, p. 18.

generated by the anti-money laundering framework has already been criticised in Chapter II at the beginning of this thesis. However, the numbers have not yet been explored in detail.

It has been established at the beginning of this chapter that the CJEU's case law in the data retention cases will be the main guide by which the measures of the Anti-money laundering Directive will be assessed. Such a comparison is not always easy, however. The system of suspicious transactions reports is the major difference between the Data retention Directive and the Anti-money laundering Directive, and where a direct comparison is difficult. The Data retention Directive allowed the competent national authorities to directly access the data collected by communication services providers. The Anti-money laundering Directive, in contrast, obliges service providers to scan all their data for "suspicious" data and to forward anything which raises a flag. Compliance with requests for information from the FIU also play a role, but the forwarding of information in the shape of a suspicious transaction report is the primary channel of the flow of information from the obliged parties to the FIU.[1744] The Data retention Directive thus applied a pull-system, and the Anti-money laundering Directive primarily applies a push-system.[1745]

At the time of writing, the newest available statistics issued by Financial Intelligence Units are from 2015. The French FIU Tracfin reports that it has received over 45 000 suspicious transactions reports in 2015.[1746] The United Kingdom UKFIU has received over 380 000 reports in the period between October 2014 and September 2015.[1747] The German FIU is the only Unit which at the time of writing has published the numbers for 2016, and it reports to have received over 40 000 reports during that year.[1748] All of the FIUs report an increase in the number of suspicious transactions reports sent in each successive year.



1744 Article 29 Working Party, Opinion 14/2011, p. 21.
1745 See also sectoin (b) of this chapter above.
1746 Tracfin annual report 2015, p. 8.
1747 NCA annual report 2015, p. 6. See for a discussion of the use of private sector information in the United Kingdom Brown (2012), p. 234.
1748 FIU Jahresbericht 2016, p. 8 f. These numbers are high at first glance. However, it should be considered that According to the *European Central Bank*, the number of non-cash payments made in these three countries amounted to ca. 62.5 billion in 2015. See ECB (2016), p. 46 (table 6).

Therefore, the difference between the Data retention Directive and the Anti-money laundering Directive may not be so great after all. Where all information the FIU could possibly wish for is immediately transmitted to it, and the FIU has on top of that the power to request any additional information if it desires further data, the situation is in effect much the same as if the FIU was granted direct access.

It should also be noted that the number of convictions for money laundering and terrorist financing is very low,[1749] and indeed it has never been high.[1750] The statistics are furthermore incomplete because although the prosecution is in principle bound to notify the FIU of the outcome of any case referred from the FIU to it, the prosecution does not always live up to this obligation.[1751] However, the German FIU registers that in less than 2% of the cases in which it does hear back from the prosecution, subsequent convictions, penalty orders, or charges are reported.[1752] The overwhelming majority of the cases are dismissed.[1753]

The low number of suspicious transaction reports that lead to a successful prosecution of a crime could be construed to argue in favour of the necessity of the measures. In fact, the low numbers of convictions compared to the large estimate of the amount of money which must in fact be laundered annually in Europe, could even support the argument that the measures now introduced are not going far enough yet.[1754]

The call for ever increasing surveillance of financial channels appears to have been heard by the European legislator, as each of the five Anti-money laundering Directives increased both the amount of obliged entities and the amount of surveillance to be carried out by those entities. The increasing surveillance measures by the increasing number of obliged parties has naturally also led to an increased number of suspicious transactions reports. This development can be followed through the statistics annually published by the national Financial Intelligence

1749 Bures (2015), p. 229 notes that the few reports on terrorist financing have been characterized by compliance officers as "just bullshit that has scared us for nothing".
1750 See the analysis of the statistics in Bures (2015), p. 227 f. See also Chapter II above.
1751 FIU Jahresbericht 2016, p. 17.
1752 FIU Jahresbericht 2016, p. 17. The FIU notes that it has never yet heard back from the prosecution about a case concerning terrorist financing.
1753 FIU Jahresbericht 2016, p. 17.
1754 See the calls for increased measures in the proposed fifth Anti-money laundering Directive, for example in European Economic and Social Committee, 13666/16, p. 3 f.

Units.[1755] However, a perusal of the statistics also shows that an increased number of suspicious transactions reports did not lead to a higher number of convicted money launderers. In the words of the European Economic and Social Committee, "Money laundering is expanding continuously in spite of the efforts made by the European and national authorities."[1756]

This lack of success is continually attempted to be remedied with an increasing extension of the anti-money laundering measures. However, this continual expansion of the elements of the crime of money laundering is deemed to be "irrational" by some commenters.[1757] The more complex anti-money laundering measures are introduced, the less effective they prove; the fewer successes of the anti-money laundering measures can be shown to have, the more powerful and sinister the underground money laundering machinery is portrayed.[1758] Therefore, ironically, the legitimacy of the continual extension of the anti-money laundering legislation is derived from its lack of success.[1759]

Considering that so few of the suspicious transactions reports indeed lead to the successful prosecution of a money launderer, and that even fewer lead to a conviction for terrorist financing, the systematic reporting of transactions, and the continual monitoring can hardly be justified. This eighth concern is therefore directly related to the first concern of the mass surveillance character of the measures. While mass surveillance measures always raise grave concerns regarding their proportionality,[1760] mass surveillance measures with so little success to justify them should almost imperatively be considered to be disproportionate. This is the eighth point flowing into the proportionality assessment of the Anti-money laundering Directive.



***(9) Requests for Information***

Besides being forwarded reports on suspicious transactions from obliged entities, the FIU may also request information from obliged entities. These requests for

1755 See, for example, FIU Jahresbericht 2016, p. 16; Tracfin annual report 2015, p. 9.
1756 European Economic and Social Committee 13666/16, p. 7.
1757 *Fischer*, quoted in Hetzer (2008), p. 565.
1758 Hetzer (2008), p. 565.
1759 Hetzer (2008), p. 565.
1760 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraphs 57-69.

information are the subject of the ninth concern connected to the anti-money laundering measures.

Although it is primarily the task of obliged entities to share information, an option for a pull-system is also provided in the Anti-money laundering Directive.[1761] In article 33 (1) (a) 4AMLD it is stipulated that obliged entities must not only forward suspicious transactions reports to the national FIU, but also further cooperate with the FIU by "promptly responding to requests by the FIU for additional information" after a report has been made. Here, the FIU is therefore not only reliant on the obliged entity's initial report alone. In addition, article 33 (1) (b) 4AMLD stipulates that obliged entities are bound to furnish "the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law." This rather openly and broadly formulated provision thus demands of obliged entities to cooperate with the FIU by forwarding all requested information.[1762] It should be emphasised that the Directive does not envisage either the option for an obliged entity to refuse such a request, nor the presence of a judicial warrant as a basis for such a request for information.[1763]

Therefore, while the Anti-money laundering Directive contains no pull-system of the same extent as the Data retention Directive did, the FIU is granted rather vast powers in the shape of requests for information.[1764] Indeed, the proposed fifth Anti-money laundering Directive is indented to extend this competence of the FIU to request information even further. Some implementations into national law stipulated that FIUs could only request information from an obliged entity if that entity had sent a suspicious activity report earlier, based on the formulation of article 33 (1) (a) 4AMLD.[1765] The proposed fifth Anti-money laundering Directive is intended to resolve this uncertainty by replacing article 33 (1) (b) 4AMLD with a shorter and clearer provision, namely "providing the FIU, directly, at its request, with all necessary information." (Art. 33 (1) (b) 5AMLD)[1766] Any uncertainties

1761 Article 29 Working Party, Opinion 14/2011, p. 21.
1762 The French FIU reports that it has issued over 25,600 requests for information in 2015. See Tracfin annual report 2015, p. 48.
1763 See also Herrmann/Soiné (2011), p. 2922 f.; Gurlit (2010), p. 1039; Roßnagel/Bedner/Knopp (2009), 540.
1764 See also EDPS Opinion 1/2017, p. 12; Article 29 Working Party, Opinion 14/2011, p. 21.
1765 COM (2016) 450 final, p. 13 f.
1766 Article 33 (1) (b) as stipulated in the fifth compromise text 15605/16 in Procedure 2016/0208/COD, of 19 December 2016.

which could be construed into the option that the obliged entity may refuse a request or comply with requests for information indirectly are thus removed, along with the reference to the procedures established by national law. This new version of article 33 would thus stipulate that (a) obliged entities must comply with requests for information which follow a suspicious transaction report, and (b) with other requests for information from the FIU, even where those were not triggered by a report from that obliged entity itself. The text of the proposed fifth Anti-money laundering Directive therefore does not leave any room for the refusal of requests for information.

In addition to the erasure of grounds on which an obliged entity might refuse requests for information, a shift of the role of the FIU can be observed. As the EDPS notes,

> "the Proposal provides that, for the future, FIUs' need to obtain additional information may no longer and not only be triggered by suspicious transactions (as is the case now), but also by [an] FIUs' own analysis and intelligence, even without a prior reporting of suspicious transactions. The role of FIUs, therefore, is shifting from being 'investigation based' to being 'intelligence based'."[1767]

This approach, as the EDPS correctly notes, will likely involve extensive data mining and Big Data analyses,[1768] to the further detriment of the privacy and data protection rights of the data subjects.[1769]

This extension of the powers and capabilities of the FIU brings the CJEU's decision in *Digital Rights Ireland* back into focus. A primary critique of the system established by the Data retention Directive was the lack of objective criteria relating to the access of retained data by the competent authorities. The CJEU criticized that the Directive



1767 EDPS Opinion 1/2017, p. 12, referring to COM (2016) 50 final, p. 7. See also Lowery (2013), p. 72; Korff (2014), p. 29.
1768 Interestingly, this concern was addressed in the Data retention Directive, in which it was stipulated that the data collected under the terms of the Directive should not be used for prevention purposes. See Maras (2012), p. 69.
1769 EDPS Opinion 1/2017, p. 12. See also Maras (2012), p. 68 f.; Leonard (2014), p. 53 ff.

> "does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the Directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto".[1770]

The CJEU therefore criticized the lack of objective substantive and procedural rules defining the conditions for access of the retained data. While in the Anti-money laundering Directive, the system is reversed, and the national authorities do not gain access directly to the retained transactions data, the critique is nonetheless applicable.[1771] Just as the Data retention Directive, the system of the Anti-money laundering Directive is marked by an absence of proper safeguards in this regard. This absence of safeguards is a strong ninth point to count into the assessment of the proportionality of the terms of the Directive.

***(10) No Notification of Data Subjects***

Closely connected to the foregoing two points is the tenth concern which is to be listed here, namely the prohibition of disclosure. Article 39 (1) 4AMLD provides that obliged entities may not inform the customer "that information is being, will be or has been transmitted in accordance with Article 33 or 34 or that a money laundering or terrorist financing analysis is being, or may be, carried out."[1772]

This prohibition of disclosure is problematic in several ways.[1773] It makes it impossible for the data subject to prevent his information from being shared with the Financial Intelligence Unit. A suspicious transactions report has the consequence that the customer will be registered by the bureaucratic machinery of the FIU, which most banking customers, including those entirely innocent of a financial crime, would certainly wish to avoid.

1770 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 61. See also Milaj/Kaiser (2017), p. 121; Bergemann (2007), p. 582.
1771 Milaj/Kaiser (2017), p. 121. See also Gietl (2010), p. 401.
1772 See, in this context, also CJEU Case C-201/14, *Bara* [2015], paragraphs 42 ff.
1773 See in this context also the detailed discussion of the rights of data subjects in Chapter V section (d).

A related problem with the prohibition of 'tipping off' the data subject of an investigation of the FIU is that the obliged party cannot fully comply with a request for information from the customer.[1774] The GDPR defines minutely which data sets the data subject has the right to access in article 15 GDPR. The list in that article also contains point (c): "the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations."[1775] The data subject's right to access the data sets stored about him ensures compliance with the principles of data protection, particularly with the principle of lawfulness, fairness and transparency (article 5 (1) (a) GDPR).

Clearly these provisions collide when a data subject, whose data has been forwarded to the FIU, exercises his rights of access.[1776] This collision is caught by article 15 (1) of the Police and Criminal Justice Authorities Directive 2016/680. According to that provision, the right of access of the data subject may be restricted by Member States

> "to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to: […] (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; […]."

As financial services providers act as processors of personal data on behalf of law enforcement agencies whenever carrying out their obligations under the Anti-money laundering Directive, this provision applies to them, negating the data subjects' right to access under the GDPR to that extent. Such a provision does not, however, automatically sanction such secrecy.[1777] In the words of the CJEU, "the fact that data are retained and subsequently used without the subscriber or registered



1774 See also recital 46 of the fourth Anti-money laundering Directive.
1775 Kaetzler (2008), p. 179.
1776 See the table of the arguments for and against disclosure as compiled by Rees/Brimstead/Smith (2003), p. 27. See also Kaetzler (2008), p. 179.
1777 Hamacher (2006), p. 636 f.; Huber (2007), p. 882; Gietl (2010), p. 401.

user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[1778]

With these words, the CJEU echoes the notion also articulated by the BVerfG in its data retention judgment. The BVerfG writes that the retention of data in the absence of suspicion against an individual can cause that individual to experience a vaguely threatening feeling of being watched, which may impact the unprejudiced exercise of this individual's rights.[1779] This threat of a chilling effect of the anti-money laundering measures is a very serious concern, which should certainly be counted into the proportionality assessment.

***(11) General Lack of Procedural Transparency***

An eleventh concern regarding the lack of transparency of the system is directly connected to the prohibition of disclosure and the potential chilling effects it may trigger.

The best way to combat such a vaguely threatening feeling of being watched would be to introduce a rigorous transparency regime.[1780] The CJEU does not go into details of how transparent the data processing must be, but the BVerfG has very clear notions of the level of transparency which would be suitable in the case of the data retention regime. According to the BVerfG, the principle of transparency as envisioned, among other documents, in article 5 (1) (a) of the GDPR, must be followed closely. This means in particular that personal data should be collected and further processed openly, that is, not in secret. Secret processing of data can only exceptionally be justified if open processing would likely frustrate the investigation for which the data was processed.[1781] While this may be the case where an operation of the secret services or a case of the protection of public or national security is concerned,[1782] it is certainly not always the case in ordinary criminal proceedings, where investigations often take place with the knowledge and even in

1778 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 37. See also Bergemann (2007), p. 585.
1779 BVerfG, 1 BvR 256/08 [2010], paragraph 212; Maras (2012), p. 74 f.; Kunnert (2014), p. 775.
1780 Article 29 Working Party, Opinion 14/2011, p. 13. See also Durner (2006), p. 214.
1781 BVerfG, 1 BvR 256/08 [2010], paragraph 243.
1782 See for the involvement of the US Secret Service in financial intelligence Lowery (2013), p. 72 ff. See also Korff (2014), p. 108.

the presence of the suspect.[1783] Therefore, a data subject can and should generally be informed about access to personal data as soon as possible.

As the BVerfG also acknowledges, there may be individual cases where secret processing of personal data is necessary. In those cases, however, a judicial order to that effect should be obtained.[1784] The urgency of the request for secret access to personal data must therefore have been proven by law enforcement agencies to the satisfaction of a judge before personal data can be secretly accessed. In addition, in such cases where the secret processing of personal data has taken place, the data subject must be informed of this processing as soon as possible.[1785] The BVerfG thus demands a high level of transparency. Due to the close similarities of the Data retention Directive with the Anti-money laundering Directive in this regard, the findings of the Court should also be applied to that Directive. This high standard of transparency, however, is directly negated by the universal obligation of non-disclosure of article 39 (1) of the Anti-money laundering Directive, and is therefore not met.

Such measures of transparency are necessary for several reasons, which are in principle the classical reasons for the need of transparency in any government decision-making process, particularly where it may affect the citizens directly. The task of such transparency measures, the BVerfG emphasises, is to protect the data subject from the situation in which his lack of knowledge of the relevance of certain data creates a threat for him.[1786] The principle of *Ignorantia legis non excusat* can only be applied if sufficient transparency measures in fact counteract such ignorance.[1787]

In addition, as the BVerfG correctly points out, hear-say and speculation can create an atmosphere of diffuse threat which should be avoided as far as possible. Instead, sufficient transparency measures also facilitate a meaningful public discussion of such measures, and can serve to cement their democratic legitimacy.[1788]

1783 BVerfG, 1 BvR 256/08 [2010], paragraph 243.
1784 BVerfG, 1 BvR 256/08 [2010], paragraph 243.
1785 BVerfG, 1 BvR 256/08 [2010], paragraph 244. See the discussion of the case law of the BVerfG in Schwartz (2012), p. 292 ff.
1786 BVerfG, 1 BvR 256/08 [2010], paragraph 242.
1787 See also Kilkelly (2003), p. 26.
1788 BVerfG, 1 BvR 256/08 [2010], paragraph 242; Article 29 Working Party, Opinion 14/2011, p. 13. See also Chapter V above.

Finally, it should be emphasised that the duty to report suspicious transactions and the obligation of non-disclosure in combination place financial services providers in a very peculiar and uncomfortable position toward their customers.[1789] They are thus paid by the customer for the (financial) services they offer, but a part of the payment also goes toward covering the considerable costs of complying with the customer due diligence obligations. The customer therefore pays the service provider not only for the provision of a service, but in addition, the customer pays for his or her own surveillance at the hands of the service provider, and must consider it a possibility that the service provider working for him or her in fact reports his or her activities to the authorities. This dual obligation of the service provider naturally places the customer and the obliged party in an almost intolerable relationship towards one another. As *Cesare Beccaria* observed as early as 1764, "Whoever suspects another to be an informer, beholds in him an enemy",[1790] which is certainly not a desirable relationship between a customer and a service provider.[1791]

This lack of transparency is the eleventh point flowing into the proportionality assessment of the terms of the Anti-money laundering Directive.

***(12) Obstruction of the Right to an Effective Remedy***

A rigorous regime of transparency does not only serve to counteract creating "in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[1792] The data subject must moreover be in a position to defend him- or herself against unlawful processing of personal data concerning him or her.[1793] Such a defence can only take place in the presence of well-defined rights of the data subject and strict transparency rules, which ensure the data subject's access to information concerning possible breaches, and allow him or her to assert and exercise his or her rights under the GDPR. In the case of secret surveillance, however, as is essentially the case in the Anti-money

1789 Schmidt/Ruckes (2014), p. 659.
1790 Beccaria (1819), p. 56. See also Constant (2003), p. 366. EDPS Opinion 1/2017, p. 14; De Hert (2003), p. 56 f.
1791 Dittrich/Trinkaus (1998), p. 346. See also EDPS (2013), p. 5; Novotny/Spiekermann (2015), p. 462.
1792 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 37. See also Dix/Petri (2009), p. 534.
1793 BVerfG, 1 BvR 256/08 [2010], paragraph 242; Article 29 Working Party, Working Document 1/2016, p. 11.

laundering Directive the lack of transparency results in a situation in which such surveillance is "essentially unaccountable"[1794] because the data subject is not in a position to defend his or her rights properly.[1795] This difficulty of defending one's rights is the twelfth concern to be considered in the proportionality assessment of the Directive.

A situation in which the data subject is essentially deprived of his rights is clearly incompatible with the right to an effective remedy and a fair trial enshrined in article 13 ECHR and article 47 of the Charter.[1796] Article 47 of the Charter protects the right to an effective remedy and fair trial:

> "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented."

In order to make use of an effective remedy, however, the data subject must be aware of access to his data, and therefore notified of it, if not before access is taking place, then at the latest as soon as the measures are concluded.[1797] The Article 29 Working Party is very clear on this point:

> "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects [an interference] can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject".[1798]

1794 Rodriguez (2011), p. 19 f. See also Göres (2005), p. 256; Hamacher (2006), p. 634; Gietl (2010), p. 401.
1795 Boehm/De Hert (2012), p. 7. See also Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 342.
1796 Article 29 Working Party, Working Document 1/2016, p. 11. See also Boehm/De Hert (2012), p. 7; Köllner/Mück (2017), p. 598.
1797 Article 29 Working Party, Working Document 1/2016, p. 11; Göres (2005), p. 256.
1798 Article 29 Working Party, Working Document 1/2016, p. 11. See also Gurlit (2010), p. 1038; Boehm/De Hert (2012), p. 4.

The Article 29 Working Party therefore in essence states that when the data subject does not learn of interferences with their rights, the right to an effective remedy effectively becomes meaningless.[1799]

The CJEU omits a detailed discussion of this point. The BVerfG, in contrast, makes it a main point in its discussion of the proportionality of the measures of the national implementation of the Data retention Directive. Importantly, the BVerfG demands that access to the retained data can in principle only be granted where the access was mandated by judicial order.[1800] Such protection by judicial order is particularly necessary where personal data is accessed secretly, without informing the data subject.[1801] While the legislator has the room to decide where such a judicial order is necessary, he is limited in this decision if the infringement of the rights of the data subjects is particularly serious. The independence of the judiciary places judges in the best position to ensure the protection of the rights of the individuals concerned.[1802]

The conditions and standards to which the judicial order must adhere are also to be strictly and specifically defined by law. High standards should be applied to the substantiation of both the request made by the law enforcement authorities to the judiciary, on which the competent court must base its decision whether or not to grant access to existing data, as well as to that judicial decision itself.[1803] The judicial order must, in accordance with the principle of proportionality, select certain clearly defined categories of data which are to be transmitted to the law enforcement agencies. A sufficiently clear judicial order will therefore discharge the service provider from conducting its own assessment, and limit both its obligation and authority to transmit only those clearly defined data.[1804] Importantly, this condition entirely rules out the option of allowing law enforcement authorities direct access to retained data.[1805]

1799 Boehm/De Hert (2012), p. 7.
1800 BVerfG, 1 BvR 256/08 [2010], paragraph 247. See also the section on requests for information above.
1801 BVerfG, 1 BvR 256/08 [2010], paragraph 248. See also Göres (2005), p. 256 f.
1802 BVerfG, 1 BvR 256/08 [2010], paragraph 248. See also Fraenkel/Hammer (2011), p. 889.
1803 BVerfG, 1 BvR 256/08 [2010], paragraph 249. See also Puschke/Singelnstein (2005), p. 3535.
1804 BVerfG, 1 BvR 256/08 [2010], paragraph 249. Note that the BVerfG has been less emphatic in this point in earlier case law. See Tolani (2007), p. 280. See also Leutheusser-Schnarrenberger (2015), p. 588.
1805 BVerfG, 1 BvR 256/08 [2010], paragraph 250. See also Göres (2005), p. 256 f.

These criteria should also be applied also to the regime of the Anti-money laundering Directive. Whether a system of suspicious transactions reports and requests for information such as envisioned by that Directive can satisfy the BVerfG's conditions in this regard is doubtful. While law enforcement agencies are not granted direct access, the Directive attempts to circumvent the need for a judicial order or similar high level of protection by demanding that obliged entities independently forward information on all suspicious activity.[1806] Therefore, while law enforcement agencies cannot directly access the retained data, the fact that all suspicious activity is forwarded to them proactively by the obliged entities in effect creates almost the same situation as if FIUs did have direct access.[1807] In addition, any further requests for information from FIUs to obliged entities are also not placed under the condition of the existence of a judicial order. This is a grave shortcoming of the terms of the Directive, which is incompatible with the demands of the BVerfG, and is unlikely to satisfy the demands of the CJEU.

Therefore, the absence of proper safeguards to protect the right to an effective remedy should be considered to be a serious weakness of the system of the Anti-money laundering Directive. It takes an important place in the proportionality assessment of the measures.

***(13) General Lack of Data Protection Safeguards***

The right to an effective remedy is not the only right that is not properly safeguarded by the anti-money laundering framework, however. General safeguards of the right to data protection are equally insufficient. This is the topic of this thirteenth point.

Chapter V of the Anti-money laundering Directive (articles 40-44 4AMLD) specifically mentions data protection in its title, "Data protection, record-retention and statistical data". However, the purpose of the provisions in that chapter is not simply to ensure the protection of the large amounts of personal data affected by the stipulations of the Directive, to guarantee that the processing of data is in accordance with European data protection legislation, or to stipulate sanctions for violations of these data protection rules. Instead, article 41 4AMLD is the only article in this chapter which concerns data protection. It reads as follows:



1806 See in this context also Korff (2014), p. 101.
1807 See also the eigth and ninth concerns discussed above.

(1) "The processing of personal data under this Directive is subject to Directive 95/46/EC,[1808] as transposed into national law. Personal data that is processed pursuant to this Directive by the Commission or by the ESAs is subject to Regulation (EC) No 45/2001.[1809]

(2) Personal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes,[1810] shall be prohibited.

(3) Obliged entities shall provide new clients with the information required pursuant to Article 10 of Directive 95/46/EC before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of obliged entities under this Directive to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of this Directive.

(4) In applying the prohibition of disclosure laid down in Article 39(1), Member States shall adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned to:

    (a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or

    (b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised."

1808 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50. Footnote added by the author.

1809 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22. Footnote added by the author.

1810 See also Kulesza (2014), p. 301 f. Footnote added by the author.

As can be seen, this article in principle repeats and applies the principle of purpose limitation and the right to information. However, it does not contain references to any of the other principles of data protection or the rights of the data subject, other than specifically restricting the right of access. Specific safeguards to ensure the security of data,[1811] the respect for the principles of data protection and the rights of the data subjects would have been highly desirable.[1812]

It is questionable, therefore, if personal data is only protected on paper or also in fact.[1813] The purpose of Chapter V of the Directive rather appears to make sure that data protection legislation does not hinder the efficient and effective processing of data in accordance with the terms of the Directive.[1814] Indeed, the EDPS states in connection with access rights to be granted in the proposed fifth Anti-money laundering Directive that they "welcome reiterated references, in the Council Position, to the need to respect data protection rules in implementing such access, but we are concerned that these statements do not translate into facts."[1815]

It has already been shown above that the Directive is entirely devoid of any protection of sensitive categories of data, which was seen as a very serious deficiency of the Directive.[1816] However, the protection of ordinary personal data is equally insufficient. The data protection safeguards currently contained in the Directive will hardly satisfy the demands of the Courts. Indeed, this is a serious concern to be considered in the proportionality assessment.

***(14) Excessive Retention Periods***

Connected to the lack of data protection safeguards is an excessive data retention period.[1817] The length of the retention period is the fourteenth concern to be addressed in this context.



The European Data Protection Supervisor is not unjustified in asking whether the statements about data protection also translates into facts, as evidenced by the

1811 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 66.
1812 See also Fuster (2016), 190 f.; Bizer (2007b), p. 588.
1813 Article 29 Working Party, Opinion 4/2014, p. 7; Article 29 Working Party Opinion 14/2011, p. 5; Fuster (2016), 190 f.
1814 Article 29 Working Party Opinion 14/2011, p. 5. See also Korff (2014), p. 101; Mezzana/Krlic (2013), p. 7 f.
1815 EDPS Opinion 1/2017, p. 11.
1816 See also the fifth concern discussed above.
1817 Clarke (2015), p. 126. See also Bizer (2007b), p. 588.

rules concerning the retention period, contained in Chapter V of the fourth Anti-money laundering Directive. The retention period is prescribed in article 40 (1) 4AMLD, setting a retention period of five years. This article describes in detail that obliged entities are responsible for retaining customer data:

> "Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:
>
> (a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;
> (b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction."

The second point is of particular interest. That a full record of transactions must be retained is a rule first introduced in the third Anti-money laundering Directive of 2005, and was retained in the current framework.[1818] Keeping a full record of transactions for such a long time frame is problematic in several ways. In the first place, the amount of transactions carried out by a single account can be immense, creating a massive amount of data which has to be stored by the financial services provider.[1819] Such storage is costly, as the data needs not only be stored, but of course stored safely in accordance with the GDPR,[1820] which is an expensive undertaking.[1821] Furthermore, it has already been mentioned that financial data is particularly vulnerable to theft and other illegitimate access. An increased retention period naturally only increases this vulnerability.

1818 See also Chapter II above.
1819 See also Roßnagel/Bedner/Knopp (2009), 538. See also the seventh concern discussed above.
1820 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 66.
1821 Roßnagel/Bedner/Knopp (2009), 538 f.

The greater problems are, however, created by the fact that such large amounts of data are stored about private individuals in the absence of any suspicion against them.[1822] The Directive makes no distinction between particular groups of persons or particular types of transactions, but instead introduces a retention regime that obliges service providers to retain all data of all customers.[1823] The sensitivity of some of the data has already been described. The complete lack of a selection, particularly concerning categories of data that might be deleted earlier for evident lack of usefulness in a potential court proceeding, is not compatible with the principle of data minimization, and raises serious questions in regard to the proportionality of such an indiscriminate retention regime.

The time frame of five years is, moreover, the minimum timeframe for storage in this context.[1824] There exist numerous additional rules concerning storage of data of legal persons, which can extend the time frame for the storage of some data concerning them. Customers may, however, also be affected by the latter part of article 40 (1) 4AMLD. After standardizing the retention period of five years in subparagraphs (a) and (b), the paragraph goes on to state,

> "Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years."



Therefore, individuals may face retention of their data of up to 10 years after the end of the business relationship. It is striking that there is thus a possibility to extend the retention period by five years in the event that a proportionality assessment comes to the conclusion that this extension is justified, but that there is

1822 See also the sixth concern discussed above.
1823 Article 29 Working Party Opinion 3/2015, p. 7; Article 29 Working Party, Opinion 14/2011, p. 23.
1824 Article 29 Working Party, Opinion 14/2011, p. 22.

no corresponding provision that would allow a shortening of the retention period in the event that a proportionality assessment comes to the conclusion that such a shortened period is justified.[1825]

The end of the business relationship is of particular moment, as the duration of the business relationship itself is not taken into account in the drafting of this provision.[1826] Individuals may well hold a bank account for years, if not decades.[1827] If a bank account is used by an individual for ten years, the customer's identification records as well as a full transaction record must be held by the financial service provider for a minimum of fifteen years. This duration of a retention period is particularly at odds with the fact that some national criminal codes have set the statutes of limitation at a much shorter time frame. In the German criminal code, for instance, money laundering falls under a statute of limitation of five years.[1828] Surely after the offence has become time-barred, there can be no justification to keep such data any longer.

However, the statutes of limitations vary considerably among Member States. Under Polish law, for example, the offence of money laundering only becomes time-barred after 15 years.[1829] In the context of the negotiations concerning the terms of the fifth Anti-money laundering Directive, the Polish government has issued a declaration in which it criticises the brevity of the retention period currently in place. It calls instead for a possibility for indefinite storage of data, at least concerning the proposed register of bank accounts (see below). "The introduction of an indefinite period for the storage of data arises from the need to ensure that the law enforcement authorities achieve the aforementioned objectives".[1830] The Polish delegation is therefore concerned that data relating to a criminal offence might be deleted before the offence is time-barred. However, in that case, it would have been much more consistent to allow for the option that retention periods follow the statute of limitation in each individual Member State. The length of the retention period would then, however, still be limited by the principle of proportionality, and an excessively long retention period will be disproportionate even in Member

1825 Article 29 Working Party, Opinion 14/2011, p. 23 f.
1826 Article 29 Working Party, Opinion 14/2011, p. 22.
1827 Article 29 Working Party, Opinion 14/2011, p. 23.
1828 According to § 78 (3) Nr. 4 juncto § 261 Strafgesetzbuch.
1829 General Secretariat of the Council, 15615/16, p. 2.
1830 General Secretariat of the Council, 15615/16, p. 2.

States with a statute of limitation of an equal amount of years. Storage of personal data for an indefinite period of time can under no circumstances be considered proportionate.[1831]

It should be kept in mind that the retention of data was of course the central subject matter of the Data retention Directive, which set the time frame for which the metadata of communications had to be retained for a period of between six and twenty-four months. The court deplores that

> "so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned."[1832]

The Court then goes on to criticize that the period of retention of the data is rigidly set rather than flexible depending on such criteria.

> "Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.."[1833]

This criticism can be applied equally to the retention periods ordered by the Anti-money laundering Directive. There is a curious lack of regard for the principle of storage limitation, set forth in article 5 (1) (e) of the GDPR.[1834] In particular the lack of a connection to the data retention period and the statute of limitation in national law, as well as the lack of any selection of which data to keep, based on "their possible usefulness for the purposes of the objective pursued or according to the persons concerned."[1835]



1831 Article 29 Working Party Opinion 14/2011, p. 22 f.
1832 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 63.
1833 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 64.
1834 Clarke (2015), p. 126 notes that the disregard for privacy is a common problem among regulators.
1835 These purposes being the p*revention, detection, investigation* and prosecution of criminal offences.

This absence of even an attempt at striking a balance is certainly objectionable. Indeed, the failure to take account of the duration of the business relationship and the subsequent possibility that data is retained for decades is an important factor to consider in the proportionality assessment of the measures of the Directive. Such a retention period of decades is almost certainly disproportionate, and based on the CJEU's judgment in the data retention cases, it cannot be expected that the Court would consider the retention period of Article 40 (1) 4AMLD proportionate.

***(15) Access to Data by Tax Authorities***

Until now, the discussion of the anti-money laundering measures has been concentrated on measures contained in the Anti-money laundering Directive itself. However, data collected, processed, and retained under the provisions of the Anti-money laundering Directive are slowly being utilized by other authorities as well.[1836] This extension of the circle of parties which are granted access to retained data and of the reasons for which access can be granted is the fifteenth concern to be discussed in this context.

Along with the proposal for a fifth Anti-money laundering Directive, the Commission has also proposed an amendment[1837] to Directive 2011/16/EU on administrative cooperation in the field of taxation,[1838] which has since been adopted as Directive (EU) 2016/2258.[1839] In its proposal, the Commission stresses that

> "it has become apparent that tax authorities need greater access to information on the beneficial owners of intermediary entities and other relevant customer due diligence information, if they are to effectively identify and address tax evasion."[1840]

When Directive 2016/2258 enters into force, the circle of entities accessing customer due diligence information is therefore increased with the inclusion of tax authorities. The amendment of Directive 2011/16/EU in essence only concerns the insertion of one paragraph, which is to read

1836 Hetzer (2008), p. 564; Göres (2005), p. 254. See also Reichling (2008), p. 672.
1837 COM (2016) 452 final.
1838 Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, OJ L 64, 11.3.2011, p. 1–12.
1839 Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, OJ L 342, 16.12.2016, p. 1–3.
1840 COM (2016) 452 final, p. 2. See also Kaetzler (2008), p. 180; Kutzner (2006), p. 644.

> "(1a) For the purpose of the implementation and enforcement of the laws of the Member States giving effect to this Directive and to ensure the functioning of the administrative cooperation it establishes, Member States shall provide by law for access by tax authorities to the mechanisms, procedures, documents and information referred to in Articles 13, 30, 31 and 40 of Directive (EU) 2015/849 of the European Parliament and of the Council".

The articles mentioned above concern customer due diligence, beneficial ownership, and retention of data. The tax authorities are therefore to gain access to all information collected on customers in the process of customer due diligence, as well as data retained on customers and transactions after the end of the business relationship with the obliged entity.

Therefore, while data has to be retained under the rules of the Anti-money laundering Directive, access to this data is already beginning to be included in other pieces of legislation.[1841] This fragmentation of laws make the legal situation increasingly difficult to assess for data subjects.[1842] In addition, the principle of purpose limitation is no longer safeguarded in this context.[1843] The EDPS finds clear words for such a situation:

> "In cases where the purposes for data processing are defined in broad or vague terms, where the data controllers have a completely different relation with the purpose pursued, both in terms of structure, resources and ability of each controller to comply with the rules in certain specific circumstances, the principle of purpose limitation is formally and substantially undermined, with the consequence that also the principle of proportionality will not be duly implemented."[1844]

The European Data Protection Supervisor therefore already hints at the conclusion that must be drawn: The extension of the circle of parties with access to retained

1841 See also Maras (2012), p. 67; Beckmann (2017), p. 974 f.

1842 See in this context also the observations on the impact of fragmentation of laws on the assessment of their legality under the provisions of the Charter as applied by the CJEU, below in Chapter X. See also Lennon/Walker (2009), p. 40 f. on function creep of the CFT rules in times of economic crises.

1843 Article 29 Working Party, Statement WP 230, p. 3; Article 29 Working Party, Opinion 14/2011, p. 17.

1844 EDPS Opinion 1/2017, p. 8. See also Fläming (2007), p. 7.

data which is practiced here by the lawmaker is a serious concern to be considered in a proportionality assessment of the measures of the Directive.

***(16) Lack of Respect for the Principle of Purpose Limitation***

The principle of purpose limitation is indeed such a central data protection principle that the discussion of it warrants its own section. The disregard for it which the lawmaker shows in the anti-money laundering framework is a sixteenth concern to be addressed in this context.

Tax authorities being granted access to the data collected under the terms of the Anti-money laundering Directive gives rise to questions concerning the respect of the principle of purpose limitation.[1845] The phenomenon that data is collected for one specific purpose and then later used for a different purpose is also known as 'function creep' or 'mission creep'.[1846] In particular data collected through measures of mass surveillance are at "risk of mission creep, because it involves the storage of large amounts of data for future use."[1847] *Boehm* and *De Hert* observe that "almost all existing databases have multiple functionalities."[1848]

It should be noted that the tax authorities are so far the only authorities being granted access on the European level, but national legislators may extend access rights to other authorities as well.[1849] This may concern access to customer due diligence and transaction information held by obliged entities or access to suspicious transactions reports and other information held by the FIU.[1850] This extension of access is a point which the European Data Protection Supervisor has also shown himself particularly alarmed about.

> "We are concerned, instead, with the fact that the Proposal introduces other policy purposes – other than countering anti-money laundering

1845 See also Hamacher (2006), p. 633 f.; Solove (2007), p. 425. See also Fläming (2007), p. 12.
1846 Hadjimatheou (2014), p. 199. See also Frasher (2016), p. 32.
1847 Hadjimatheou (2014), p. 200. See also United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), p. 21 f.
1848 Boehm/De Hert (2012), p. 2. See also Chapter V above and Chapter X below.
1849 See for instance the table of users with "'direct' access" in NCA annual report 2015, p. 40. See also *Huber's* concerns about access being granted to secret services: Huber (2007), p. 881 ff.
1850 See NCA annual report 2015, p. 40. Note that the report does not make it clear how far these access rights extend precisely.

> and terrorism financing[1851] – that do not seem clearly identified and, therefore, raises questions as to why certain forms of invasive personal data processing, acceptable in relation to anti-money laundering and fight against terrorism, are necessary out of those contexts and on whether they are proportionate."[1852]

The EDPS means that the fight against serious crime is a strong objective in the public interest, for which certain interferences with the rights of the population can be tolerated and considered proportionate. Other objectives in the public interest may not be considered quite as important, and may not stretch to justifying the same interferences as the fight against serious crime might justify.[1853] However, once the database exists, the threshold for secondary use of collected data is significantly lowered. Indeed, it is often considered that the mere existence of certain databases will inevitably lead to the demand that more and more authorities should be granted access to those databases.[1854] This is usually the case where the secondary purposes are of a minor importance as a legitimate purpose than the primary purpose for which the database was originally created. It should also be pointed out in this regard that the general tasks of law enforcement as such cannot be counted as being "one specified, explicit and legitimate purpose."[1855] Therefore, each purpose for which existing data collections are to be accessed by law enforcement agencies should be considered and assessed individually to determine whether or not the urgency of the purpose can justify the access.

There is some danger, therefore, that data originally proportionately collected and processed for an important public interest are then released to be used for other policy considerations which in themselves could not have justified the collection and processing of this data.[1856] This threat is recognised and deplored



1851 Sic, but the EDPS clearly means to say "countering money-laundering and terrorist financing". Footnote added by the author.

1852 EDPS Opinion 1/2017, p. 8. See also Article 29 Working Party, Opinion 14/2011, p. 14, 17.

1853 Maras (2012), p. 67; Dix/Petri (2009), p. 533. See also Beckmann (2017), p. 974 f.

1854 Reichling (2008), p. 672. *Reichling* deplores this development in the context of both financial data as well as street toll data. See also Chapter X below.

1855 Article 29 Working Party Opinion 3/2015, p. 6.

1856 See particularly NCA annual report 2015, p. 26 ff. Note that in that report, money laundering and terrorist financing are only two considerations among many, and apparently not the most important ones, in the assessment of suspicious activity reports. See also Carlé (2007), p. 2226; United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014), p. 9.

by the EDPS,[1857] who stresses the many different purposes for which data collected under the proposed fifth Anti-money laundering Directive are to be processed. The Supervisor observes that

> "we notice that under the new provisions, personal data would be processed for a number of purposes: countering anti-money laundering and terrorism financing; countering tax evasion (and elusion); preventing financial crimes and/or abuses of the financial markets; enhancing corporate transparency (necessary, in turn, to protect minority shareholders of corporations as well as any third party doing business with such corporations); give governments and regulators the opportunity to respond quickly to alternative investment techniques; allow public scrutiny on the functioning of financial markets, on investors and on tax evaders."[1858]

The judgment of the EDPS, based on the identification of these varied different purposes, is annihilating:

> "Processing personal data collected for one purpose for another, completely unrelated purpose infringes the data protection principle of purpose limitation and threatens the implementation of the principle of proportionality."[1859]

Not only the purposes for which this data is processed are very varied, but there are also a large number of different controllers and processors involved, which carry out these different processing tasks. Concerning those different controllers, the EDPS is concerned that the controllers apply "different 'standards', in terms of ability to comply with data protection rules, or may carry out data processing which is not proportional to the purpose sought."[1860] In the presence of all this uncertainty concerning the purposes and the amount of data processing to be carried out, and the large possible variety in data controllers involved, one cannot but agree with the EDPS that the principle of purpose limitation is gravely endangered.

1857 EDPS Opinion 1/2017, p. 9; Article 29 Working Party Opinion 14/2011, p. 7, 17.
1858 EDPS Opinion 1/2017, p. 9.
1859 EDPS Opinion 1/2017, p. 9. See also Hamacher (2006), p. 634; Weichert (2015), p. 19.
1860 EDPS Opinion 1/2017, p. 9.

This uncertainty concerning the principle of purpose limitation is also not alleviated in the text of the proposed fifth Anti-money laundering Directive. The fifth Compromise Text of the Directive attempts to sharpen the focus again on the purpose of a fight against money laundering and terrorist financing, leaving the policy goal of fighting tax evasion and avoidance aside. In this way, the first three recitals very clearly set out the aims and purposes of the Directive, describing it as an important primary tool against money laundering and terrorist financing (recitals 1-3 5AMLD). However, the fact that the recitals refer to the fight against money laundering as the primary purpose of data processing does not take away the fact that access rights are granted to entities for other purposes. Therefore, while references to the policy goal of fighting tax evasion and avoidance have been largely removed and avoided in the text of the Directive, the fact that the information collected under the Directive are also used for this purpose a fact and must be emphasised.[1861]

This disregard for the principle of purpose limitation is another strong point which must be made against the proportionality of the Anti-money laundering Directive.

***(17) Additional Proposed Rules***

Finally, the seventeenth point to be discussed in this regard are proposed future amendments contained in the proposal for a fifth Anti-money laundering Directive. The proposal for the fifth Anti-money laundering Directive contains the statement that

> "The proposed amendments to the 4AMLD (and Directive 2009/101/EC)[1862] are in line with policy aims pursued by the Union, and in particular […] the reformed data protection regime, stemming from Regulation



1861 See above, and COM (2016) 451 final, p. 5 f.

1862 Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (Text with EEA relevance), OJ L 258, 1.10.2009, p. 11–19. Footnote added by the author.

> (EU) 2016/679[1863] and Directive (EU) 2016/680,[1864] and in line with the relevant case law of the Court of Justice of the European Union".[1865]

Interestingly, despite this statement, the proposal then does nothing to alleviate any of the grievances listed in the previous seventeen sections. Instead, it contains two particular provisions which, if they were to be passed in the shape they take in the proposal, could be added to the list of issues above.[1866] Both essentially concern a strengthening of the data access capabilities of the FIUs.

In the first place, the Commission is concerned about the fact that in some Member States, FIUs do not have full and complete access to information.[1867]

> "That information is currently limited in certain Member States by the requirement that a prior suspicious transaction report has first been made by an obliged entity. FIUs should be able to obtain additional information from obliged entities, and should have access on a timely basis to the financial, administrative and law enforcement information they require to undertake their functions properly even without there having been a suspicious transaction report."[1868]

The reason the Commission gives for this extended scope is the need to comply with the newest international standards.[1869]

---

1863 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88. Footnote added by the author.

1864 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131. Footnote added by the author.

1865 COM (2016) 450 final, p. 5.

1866 See in this context also Article 29 Working Party Opinion 14/2011, p. 11.

1867 See also the section on requests for information above.

1868 COM (2016) 450 final, p. 14.

1869 See also the remarks made on the conflict between the protection of privacy and personal data and the anti-money laundering standards in section (i) below.

The Commission does point out that Member States are going to be free to define conditions for access other than the fact that no suspicious transaction report has been made, as well as "effective and proportional rules" concerning the processing of information received without a prior report, and finally repeats that the FIUs are bound to rules concerning confidentiality and data security.[1870]

However, this statement of the Commission is not convincing. For instance, as has been discussed in the ninth concern above, the rule that an FIU can only request information from an obliged entity if that entity has previously filed a suspicious transactions report is not an unreasonable rule in the interest of the respect for the principle of proportionality. Yet, Member States are to be barred from introducing such a limitation with this amendment of the Directive. This response begs the question what options the Member States then have to introduce 'effective and proportional rules' concerning the conditions for access to data and to effectively limit the powers of the FIU in the interest of privacy and data protection and the principle of proportionality. It would appear that any limitation a Member State might introduce is incompatible with the very wide access Member States are bound to grant FIUs to customer data. This lack of potential limitations to access under national law aggravates the situation outlined above regarding concerns about the presumption of innocence and transparency.

In the second place, the FIUs are also to be granted easier access to information on holders of bank accounts. In this case, the Commission extends a recommendation of the fourth Anti-money laundering Directive to a binding provision. In recital 57 of the fourth Anti-money laundering Directive, Member States were recommended to set up a national information system containing the population's bank account information, but not all Member States have followed this call.

> "As not all Member States have mechanisms in place allowing their FIUs to have timely access to information on the identity of holders of bank and payment accounts, some FIUs are hampered in the detection of criminal and terrorist financial flows at national level. Moreover, the FIUs concerned are also unable to exchange such information with their EU and non EU-counterparts, which complicates cross-border preventative action."[1871]

1870 COM (2016) 450 final, p. 14.
1871 COM (2016) 450 final, p. 14. See also Göres (2005), p. 254; Hamacher (2006), p. 636 f.

Member States are thus required to "set up a central registry, containing the necessary data allowing for the identification of holders of bank and payment accounts, and granting their own national FIUs and AML/CFT competent authorities a full and swift access to the information kept in the registry", or to set up a differently organised system to achieve the same effect.[1872] The Commission believes that the establishment of such a system "will lead to a faster detection – both nationally and internationally – of suspicious ML/TF transactions, and improve preventive action",[1873] although it is unclear on which facts this conviction is based.

The proposal of this measure is also accompanied by statements concerning the protection of personal data. It is left up to the Member States to define the conditions under which the authorities can access that database.[1874] However, in a repetition of what was said above, it is unclear how meaningful conditions can be installed if Member States are under the obligation to ensure that the authorities are granted such "full and swift access".[1875] Such full and swift access appears to be incompatible with any meaningful and effective safeguards for privacy and data protection.

Furthermore, the Commission does implicitly refer to the principles relating to the processing of personal data, particularly to the principle of data minimization and storage limitation. It requires that the data subjects must be informed of this processing, and that they are given the chance to access data about them and remedy errors if needed.[1876] The European Economic and Social Committee appears, in its opinion on the draft of the fifth Anti-money laundering Directive, to recognise this issue, and "suggests that the Commission should explore additional steps to protect the rights of citizens against illegal use or abuse of the information recorded by the competent authorities or obliged entities",[1877] but it does not suggest how such additional steps might be shaped. In the absence of precise conditions, and in the face of the obligations on Member States to grant access to data, the

1872 COM (2016) 450 final, p. 14.
1873 COM (2016) 450 final, p. 14.
1874 Cf. BVerfG, 1 BvR 256/08 [2010], paragraph 254 ff.; Göres (2005), p. 254.
1875 COM (2016) 450 final, p. 14.
1876 COM (2016) 450 final, p. 14 f.
1877 European Economic and Social Committee 13666/16, p. 5. See also Göres (2005), p. 254.

statements of the Commission can therefore hardly be considered to be more than declaratory in nature.[1878]

In addition to the bank account registry which is to be introduced as mandatory by the fifth Anti-money laundering Directive, the Commission is also considering a similar registry for users of virtual currencies. The Commission is proposing a structure of three measures to include virtual currencies into the scope of the fifth Anti-money laundering Directive, namely

> "(i) bringing virtual currency exchange platforms and (ii) custodial wallet providers under the scope of the Directive, while (iii) allowing more time to consider options as regards a system of voluntary self-identification of virtual currency users."[1879]

The first two amendments, by which exchanges and wallet providers are to be brought under the scope of the Directive have already been discussed in Chapter IV of this thesis above. In principle, those two measures are to be regarded as a logical step which may bring virtual currency service providers more legal certainty and help to integrate them into the financial service industry.

The final option of a system of self-identified users of virtual currencies cannot be considered to be a reasonable step, however.[1880] A database of identified users of the virtual currency system would be a very serious threat to the privacy of any user of the system.[1881] The identified users would face their transaction history being linked directly to them, which would entirely deprive them of privacy in this regard. In addition, the privacy of any unidentified users would be in jeopardy, as the identification of other users makes any unidentified user more vulnerable to linking of information, and to having their identities discovered by connecting their transactions to identified users who may be in possession of information concerning them. It is unclear how the virtual currency community would respond to the introduction of such a database. However, considering the statements that have been made in Chapter III of this thesis above on the background of large parts of the community, it is likely that the introduction of such a database would trigger

1878 See in this context also Boehm (2012), p. 341 f.
1879 COM (2016) 450 final, p. 9.
1880 See also Chapter VI above.
1881 Reid/Harrigan (2014), p. 15.

rather radical responses in the virtual currency environment, of both a technical as well as of an ideological nature. In any case, such a scheme of voluntary self-identification is unlikely to be successful.

Finally, it should be repeated that the connection to Article 114 TFEU as a legal basis is very thin and is increasingly weakening with the proposed fifth Directive.[1882] General concerns about the validity of the legal basis of the fourth Anti-money laundering Directive have already been explained above. The recitals of the proposed fifth Anti-money laundering Directive enhance those concerns. The first recital, for instance, which in directives is usually reserved to establishing the connection to the legal basis, appears to focus very much on the intended criminal law nature of the amendments. It reads,

> "Directive (EU) 2015/849 of the European Parliament and Council constitutes the main legal instrument in the prevention of the use of the Union's financial system for the purpose of money laundering and terrorist financing. That Directive, which is to be transposed by 26 January 2017, sets out a comprehensive framework to address the collection of money or property for terrorist purposes by requiring Member States to identify, understand and mitigate risks related to money laundering and terrorist financing."[1883]

Therefore, the text of the proposal does not alleviate any of the concerns expressed in the sixteen previous sections. In fact, it increases the seriousness of some of the interferences identified in the system of its predecessor. However, the fifth Anti-money laundering Directive is currently still under discussion and its precise final terms and scope is not yet clear. The following proportionality assessment will therefore be based on the text of the fourth Anti-money laundering Directive, but it will be valid not only for that Directive, but also for the amendment.

1882 See also Hornung/Schnabel (2009b), p. 119; Gietl/Tomasic (2008), p. 800.
1883 COM (2016) 450 final, p. 21.

## i. Results

Each of the concerns explained above shows a distinct weakness of the Anti-money laundering Directive. All of the seventeen concerns taken together argue the disproportionality of the Directive very clearly.

There are several ways in which the measures could be made less intrusive into the financial privacy of the population of Europe. They have been discussed individually in detail above and shall here only be summarised briefly, in the order of their appearance in this chapter. In the first place, the scope of the Directive goes beyond what is necessary by including in its definition of the predicate offences to money laundering a catch-all provision which includes also crimes which cannot be considered serious. Secondly, the Directive fails to create meaningful exceptions for categories of people who can be exempted from the customer due diligence regime. Monitoring of transactions in the absence of any suspicion against the customer clearly goes beyond what is necessary in order to curb money laundering and terrorist financing. In the third place, options for anonymous use of the services of obliged entities should be retained. This concerns in particular small service providers which do not establish a long-term business relationship with the client. In the fourth place, the customer must be informed promptly of access to his personal data by the FIU. This access should furthermore only be granted in the presence of a judicial order. Finally, the retention periods stipulated by the Directive go beyond what is necessary. Data should only be retained if, and insofar as they relate to suspicious activity or where a data subject or transaction has been connected by the law enforcement authorities to serious crime. In addition, even customer data relating to suspicious activity must be deleted at the latest as soon as the period of limitation has passed. All other data should be deleted as soon as they are no longer necessary for the service provider in the ordinary course of business.



The Article 29 Working Party in fact goes beyond this assessment to make a general statement tying proportionality to the principles of data protection, particularly the principles of data minimisation and purpose limitation. It sums up its assessment by simply stating that "Under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirement

of necessity and proportionality set out in these data protection principles."[1884] This view is shared in this thesis.

**i. Assessment of the Proportionality According to the Standards Applied by the CJEU**

As has been shown, the CJEU applies a three-tier proportionality test, according to which the measures in question must be suitable, necessary, and proportionate *in stricto sensu* to achieve a legitimate aim. The legitimate aim and the suitability have already been discussed in detail above, and the judgment on the necessity and the proportionality *in stricto sensu* of the measures could be based on the seventeen concerns about the Directive that were just listed.

An assessment of the seventeen grounds for concern that have been listed above leaves no doubt that the measures of the Directive go far beyond what is necessary and reasonable according to the standards applied by the CJEU.[1885] In particular the unlimited scope of the Directive and the absence of meaningful data protection safeguards are two points on which alone a negative proportionality assessment can be based. The excessive retention period should be valued to be of equal fatality.

This assessment is directly based on the Court's own case law, particularly the data retention cases, in which the CJEU made the oft-quoted statement that

> "while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight."[1886]

The Court then continues to point out that

1884 Article 29 Working Party, Opinion 4/2014, p. 6.
1885 See also EDPS Opinion 1/2017, p. 11: "we still consider that the implementation of the fundamental principle remains unclear", meaning the proportionality of the proposed fifth Anti-money laundering Directive.
1886 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 103. See also Dittrich/Trinkaus (1998), p. 347; Tridimas (1999), p. 77; Solove (2007), p. 411.

> "In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.
>
> Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy […].[1887]
>
> Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime".[1888]



The same applies to the Anti-money laundering Directive. As access to financial services is of the utmost importance for the average member of the population in the European Union, particularly in those Member States in which the digitalization of payments is advancing rapidly, all use of the financial services of the population is comprehensively mapped out and monitored by obliged entities

1887 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 104-105. See also CJEU Case C-305/05, *Ordre des barreaux francophones et germanophone and Others v Conseil des ministers* [2007]. Footnote added by the author.
1888 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 106.

on behalf of the Financial Intelligence Units. This constant and comprehensive monitoring creates a situation in which the population's rights to privacy and data protection are subject to a constant serious interference.[1889]

The complete lack of meaningful personal or material exceptions to this monitoring additionally make this interference particularly serious. Each customer of financial services is in effect under the suspicion of potential involvement in crime. This is of particular moment as the principle of proportionality in connection with the rule of law also demand that the intensity of the interference with fundamental rights is in proportion to the intensity of the suspicions raised against a certain individual.[1890] This means that a serious interference with a person's rights may in principle only take place in the event that a strong suspicion is levelled against a certain person.[1891] Blanket measures interfering with the rights of the population at large can therefore generally not be reconciled with the rule of law and must therefore always be rejected as disproportionate. In the words of *Vassilios Skouris*,

> "General preventive measures, which allow the authorities to collect data massively, to evaluate it in detail, and to communicate it indiscriminately, in the absence of a specific reason or a direct reference to specific persons, are not compatible with the system of fundamental values which are peculiar to the European Union, and which characterize this unique international organization."[1892]

Therefore, the character of mass surveillance which the anti-money laundering measures assume, and the complete lack of a limitation in scope as to the data that is being processed, is outright incompatible with the principle of proportionality.

The Anti-money laundering Directive thus introduces measures of mass surveillance, covering every member of the European population who accesses financial services, and intruding thereby severely into every individual's private lives, including into sensitive and intimate areas of their private lives. On the other hand, there is the fight against two particular financial crimes, money laundering and terrorist financing.

1889 Article 29 Working Party, Opinion 14/2011, p. 26.
1890 Hamacher (2006), p. 635; Barak (2013), p. 226 ff.
1891 Hamacher (2006), p. 635.
1892 Skouris (2016), p. 1364. See also Hirsch (2008b), p. 89 f.

The measures taken against money laundering and terrorist financing are tools intended to curb the offences related to these crimes. In the case of terrorist financing, it is the terrorist organizations and the commission of terrorist attacks which are to be hampered by the prohibition of forwarding financial support to such groups. In the case of money laundering, the idea that the perpetrator of any crime should not financially benefit from that crime is something that everyone can probably agree on.[1893] Furthermore, the predicate offences of money laundering are to be made less attractive and simultaneously easier to detect with the help of the anti-money laundering rules. The interests that are pursued by the measures of the Directive are therefore certainly legitimate.

The translation of this legitimate interest in curbing those crimes into legal rules, however, has not been carried out without difficulty. In both cases there is reasonable doubt about how much the fight against the financial crimes in fact impacts the related offences. The crime statistics have not yet reflected either a decrease of the commission of crimes or of the size of the underground economy, or an increase of the number of convictions and solved cases. It is certainly a reasonable question to ask, whether the resources currently invested in the fight against money laundering and terrorist financing on the basis of the Directive were not better reinvested directly in the fight against the predicate offences to money laundering or in the detection and prevention of terrorist activity in Europe.[1894]

In addition, the reporting obligations falling on the entire financial sector are marked by the complete intransparency of what types of behaviour may give occasion to a suspicious activity report.[1895] The situation is aggravated by the fact that data is accessed without the data subject being notified. This lack of a notification in turn bars the data subject from any possibility to prevent or challenge unlawful processing.[1896] In the words of the CJEU, "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[1897]



1893 Trüg (2017), p. 1913 ff.
1894 See Chapter II above.
1895 See in this context also NCA annual report 2015, p. 19 f.
1896 Boehm/De Hert (2012), p. 4 f. See also Baum/Hirsch/Leutheusser-Schnarrenberger (2017), p. 342.
1897 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 37.

Finally, the retention period is set at five years, and may be extended to ten years after the end of the business relationship, which, in the case of a credit institution, may potentially last decades. The Directive furthermore fails to determine categories of data which can be deleted before this time.

In sum, the measures of the Anti-money laundering Directive fail to comply with the principles of data protection, specifically the principle of lawfulness, fairness and transparency, the principle of purpose limitation, the principle of data minimisation, the principle of storage limitation, and the principle of accountability.[1898] The Directive very seriously interferes with the rights to privacy and data protection, as well as the right to a fair trial. Based on the foregoing, the measures of the Anti-money laundering Directive are not limited to what is necessary to achieve the aim of fighting serious crime. Nor is the lawmaker successful in striking a balance between the intrusion into the rights to privacy and data protection and the benefit of the measures to the public interest in potentially more effective investigations into money laundering and terrorist financing; the costs in terms of a loss of privacy and the protection of personal data are not in accord with the potential gains. The interferences with the fundamental rights of the data subjects are of such a magnitude that they cannot be deemed proportionate to the aim pursued.

Based on this list of serious shortcomings of the Directive, and supported by the CJEU's case law, the Directive's claim to proportionality must be rejected.[1899]

**ii. Assessment of the Proportionality According to the Standards Applied by the ECtHR**

It is the CJEU which is to judge on the proportionality of any European Directive. However, the importance of the ECtHR's case law in the development of the principle of proportionality and the high regard the CJEU is showing for the ECtHR's jurisprudence warrants a further assessment of the principle of proportionality as applied by the ECtHR. In addition, it has been shown that the Anti-money laundering Directive is one item in a network of national and international legal instruments which have together generated the approach described and specified by the Anti-money laundering Directive. The anti-money laundering approaches followed in numerous countries outside of the European Union are following a

1898 Monteleone (2012), p. 19 f. See also Macnish (2012), p. 178.
1899 See also Article 29 Working Party Opinion 14/2011, p. 8.

very similar strategy, based on the international instruments by which states are directly and indirectly bound. Coupled with the different criteria for accessibility of the ECtHR compared to the CJEU, it is not impossible that the ECtHR will be called upon to adjudicate on a case concerning the violation of article 8 ECHR by the anti-money laundering measures.

The proportionality assessment of the anti-money laundering measures by the ECtHR would be of great interest in the first place to European states outside of the European Union and therefore outside of the sphere of influence of the Charter. In those states, the ECHR is the main international human rights document which can be applied in order to defend the right to privacy; the ECtHR applying the ECHR is therefore of even greater importance there than in European Union Member States. In the second place, it would have a great impact on Member States of the European Union as well. They would be forced by a negative proportionality assessment of the anti-money laundering approach by the ECtHR to exercise their influence on the international anti-money laundering strategy to enforce a redesign of the system, with better added data protection and privacy safeguards. Such an improved privacy and data protection standard in the international anti-money laundering strategy would be of particular benefit and moment to states not covered by either the Charter or the ECHR, as it may result in more nuanced international standards rather than forcing all states to apply one specific blunt approach. Finally, the ECtHR is in some cases more accessible to the citizens of a Member State of the European Union than the CJEU. While access to the CJEU depends on the referral of a case by the national court and is narrowly circumscribed by the questions the national court formulates, the ECtHR can be accessed by individuals on their own initiative after exhausting domestic legal remedies.



Applying the principles applied by the ECtHR to determine what is necessary in a democratic society, the measures of the Anti-money laundering Directive fall equally short of the Court's demands, and would not satisfy the proportionality standards demanded by it. According to the case law of the ECtHR,

> "An interference will be considered necessary in a democratic society for a legitimate aim if it answers a 'pressing social need' and, in particular, if it

> is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities are 'relevant and sufficient'."[1900]

The legitimacy of the aim has been addressed at the beginning of this chapter in some detail, and it is in principle not disputed that the fight against money laundering and terrorist financing is an important policy goal. Also the relevancy and sufficiency of the reasons given for the introduction of the Anti-money laundering Directive is conceded.

However, the question whether the Anti-money laundering Directive answers a "pressing social need" is more difficult to answer. This issue is aggravated by the fact that the term of a pressing social need is not yet conclusively defined by the ECtHR in its case law. However, it is clear that this term requires the existence of a high "level of severity, urgency or immediacy associated with the need that the measure is seeking to address."[1901] The ECtHR has not yet had the opportunity to share its views on the urgency of the objective of fighting money laundering and terrorist financing, but it is likely that the Court would be willing to accept that measures intended to curb money laundering and terrorist financing as a sufficiently pressing social need to satisfy this criterion.

However, these two criteria are most related to the justification of the measures. In addition, the ECtHR demands that the design of the measures taken is undertaken with the necessary care. Indeed, the ECtHR's case law on surveillance gives a clear indication of the disproportionality of the anti-money laundering measures. The most pertinent test applied by the ECtHR in this context is the question whether there are adequate and effective safeguards against abuse.[1902] In its early decisions in *Klass* and *Leander,* the ECtHR established that

> "in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse".[1903]

1900 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 101.
1901 Article 29 Working Party, Opinion 1/2014, p. 7; Barak (2013), p. 277 f.
1902 ECtHR Case of *Leander v. Sweden* [1987], paragraph 60.
1903 ECtHR Case of *Leander v. Sweden* [1987], paragraph 60.

In the case of the Anti-money laundering Directive, the measures in question concern different types of data processing. The adequate and effective safeguards that are needed in any data processing operation are those of strong data protection guarantees, implementing the principles of data protection and safeguarding the rights of the data subject. In particular, sensitive data should be protected from illegitimate access and processing. It has already been shown in the previous sections that the safeguards contained in the Anti-money laundering Directive are inadequate.

The safeguards contained in article 41 4AMLD contain insufficient guarantees to ensure a high standard of data protection throughout all of the data processing operations carried out pursuant to the terms of the Anti-money laundering Directive. The situation is exacerbated by the fact that the Directive contains no safeguards at all for sensitive data. On the contrary, the terms of the Directive are so starkly in opposition to the principles of data protection that in fact it does not appear to be possible reconcile the measures of the Anti-money laundering Directive with the principles of lawfulness, fairness and transparency, the principle of purpose limitation, the principle of data minimisation, and the principle of storage limitation (article 5 C108). Any legislation on data processing so entirely in dissonance with these fundamental principles of data protection cannot be deemed to contain adequate and effective guarantees against abuse.

Therefore, as the measures of the Anti-money laundering Directive are not limited by almost any safeguards, the demand of the ECtHR that such legislation must be accompanied by "adequate and effective guarantees" is not met. The terms of the Directive therefore do not meet the standards applied by the ECtHR.



**iii. Invalidation of the Directive**

When the CJEU finds a legislative act of the European lawmaker to be in excess of the limits of the proportionality principle, that act is generally invalidated. [1904] The Data retention Directive was also invalidated in this way by the Court in the *Digital Rights Ireland* judgment.[1905] The Directive thus ceases to develop any legal effects, and the Member States are released from their obligation to implement

1904 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 69.
1905 Kunnert (2014), p. 778.

the Directive into national law. This would be the consequence of a successful challenge to the measures of the Anti-money laundering Directive as well.

The Court does have milder sanctions at its disposal for measures which can be bent into proportionality by the lawmaker with relative ease. In such cases, the Court may demand amendments to the measures rather than invalidating them outright. However, such a milder sanction can hardly be applied in the case of the Anti-money laundering Directive. The approach to anti-money laundering rests entirely on measures of mass surveillance and extensive data processing by obliged entities and FIUs. The complete coverage of all potential avenues for money laundering and terrorist financing and the equally complete coverage of all customers and transactions is the key concept of the anti-money laundering approach ordered by the Directive. Therefore, any demands by the CJEU to amend the mass surveillance character of the measures would have essentially the same effect as invalidating it outright:[1906] The approach would no longer be viable. In addition, the CJEU's recent case law gives a clear indication that the Court has chosen to pursue a very strict approach to the protection of data protection and privacy, and that it is willing to use the heavy ordnances in its arsenal for the protection of these rights.

Therefore, based on the seriousness of the interferences with the rights to privacy and data protection caused by the sweeping surveillance measures of the Anti-money laundering Directive, and on the line of case law in which the CJEU has not hesitated to invalidate instruments it considered inadequate, no other outcome of a proportionality assessment of the measures of the Anti-money laundering Directive than the invalidation of the Directive can be expected or indeed desired.

The national implementation of the anti-money laundering measures is a different matter, however. The invalidation of the Data retention Directive has not automatically invalidated the national laws implementing the Directive.[1907] In several Member States, the implementation had already been challenged before the national courts, with the result that the implementing acts had been invalidated. Several countries found themselves therefore technically in breach of

1906 See in this context also Beckmann (2017), p. 975.
1907 Article 29 Working Party, Statement on the data retention judgment (WP 220), p. 2. See also Kunnert (2014), p. 778; Forgó et al. (2008), p. 681.

their obligation to transpose directives into national law. Germany, for instance, found itself in that situation after the BVerfG invalidated the legal provisions implementing the Data retention Directive into national law. Other countries retained their national implementation of that Directive.

In the *Digital Rights Ireland* judgment, the CJEU only discussed the proportionality of the Data retention Directive, and only judged the validity of that Directive. National implementations did not play a role in this judgment, and have not played a role in other comparable decisions on the validity of European directives. The national implementations of the Data retention Directive were not invalidated by the CJEU's judgment, and in some Member States the national provisions implementing the Data retention Directive are still valid.[1908]

Whether a national law based on a directive that was deemed in excess of the limits of the proportionality principle can preserve its validity is in principle left to the national courts to decide. A survey of the decisions of the national courts before which the national implementations of the Data retention Directive were challenged shows that most European countries share common expectations of proportionality and protection of the rights to privacy and data protection. The national courts have overturned all or parts of the national implementation of the Data retention Directive wherever challenged.[1909] The similar judgments in the data retention cases brought before national courts before and after the CJEU's own ruling makes it clear that in most Member States, a common horizon of privacy and data protection is accepted and maintained.

In addition, the CJEU's decision in *Tele2 Sverige* has made it clear that if national laws are challenged before the CJEU, the Court will apply the same standards to interferences by national law as to interferences by European law. Therefore, whenever a directive is invalidated by the CJEU on the ground that it "exceeded the limits imposed by compliance with the principle of proportionality", a national law closely based on that directive cannot be expected to be assessed with a different result.



1908 See the overview of national data retention legislation and amendments after the Digital Rights Ireland judgment in FRA (2016).
1909 See the summary of data retention laws in the individual Member States at FRA (2016).

**iv. Increased Judicial Protection**

The invalidation of the legal basis for the anti-money laundering measures would naturally put a stop to the obligations conferred thereby upon the obliged parties. This removal of a large part of the obligations would benefit in the first place the data subjects, who would regain an important aspect of their privacy. But the revocation of the obligations would also be of a significant economic advantage for service providers.

The removal of the obligation to identify would benefit small service providers and sellers of high-value goods particularly, as these service providers would often not need to identify customers in the course of their business transaction with the customer. Similarly, the removal of the obligation to monitor would be of significant benefit for smaller service providers as well as the larger businesses. Finally, the obligation to retain data would equally be of particular benefit to smaller service providers. Larger financial service providers, particularly banks, keep data for a certain period of time in any case, also for the convenience of customers.

The reporting obligations especially would be lifted from obliged entities. The consequence would have to be a return to the warrant system. As with requests for information directed to service providers of other industries about their customers, law enforcement authorities would have to first form a suspicion against a certain individual, and then secondly obtain a warrant for each access to personal data collected by private entities.[1910] The warrant would furthermore have to comply with high standards. In the application for a warrant, the seriousness of the suspected criminal offence would have to be shown by the law enforcement authorities to the court. In particular, the data desired by law enforcement agencies would have to be defined narrowly and explicitly. That way, all obliged entities would be discharged from the obligation to study, define, and monitor suspicious activity themselves.

In sum, large amounts of data could be deleted by service providers, but it should not be forgotten that much data would be retained by the service providers in the ordinary course of business. A bank, for instance, will certainly retain data on

1910 See Hamacher (2006), p. 636 f.; Korff (2014), p. 104 f.; Herrmann/Soiné (2011), p. 2924 f. See also Singelnstein/Derin (2017), p. 2647.

customer transactions for some time, in order to provide a secure service to its customers.[1911] This data retained in the ordinary course of business would certainly still be available to law enforcement agencies upon presentation of a judicial order granting them access. Quick-freeze processes in order to prevent data on specific persons from being deleted may also be explored as an option.[1912] Making a judicial warrant a mandatory condition for access to retained data would also be in line with the case law of the CJEU, the ECtHR, and the BVerfG.[1913] The current system of placing firstly the obligation to monitor and report on all financial services providers, and secondly to obey all requests for information from the FIU in the absence of a judicial order, can under no circumstances be maintained.[1914]

**v. Conflict with the FATF Standards**

It has been argued above that the CJEU would have to follow its own reasoning in the *Digital Rights Ireland* judgment when reviewing the validity of the Anti-money laundering Directive and therefore come to the conclusion that this newer Directive displays the same weaknesses which were deemed disproportional in the earlier Data retention Directive. The consequence would be the invalidity of the Anti-money laundering Directive. However, despite the same classification of the material provisions as disproportional and despite the same conclusion of invalidity of the Directive, the tangible consequences of the invalidity of the Anti-money laundering Directive and the Data retention Directive would be different in one significant way. The fact that the Anti-money laundering Directive is the implementation of the FATF's international standards[1915] makes this subject matter much more politically explosive than the data retention complex was.

The FATF and its work have already been introduced in earlier chapters.[1916] The Financial Actions Task Force is an international body concerned with anti-money laundering and countering the financing of terrorism, which is marked in particular by its power to periodically examine the anti-money laundering laws of members and non-members alike and judge the conformity of these laws



1911 See also Chapters II and VII above.
1912 Kunnert (2014), p. 783; Brunst (2011), p. 620; Bizer (2007b), p. 588.
1913 Article 29 Working Party, Working Document 1/2016, p. 9 f.
1914 See in this context also Korff (2014), p. 101.
1915 The same of course applies to the proposal of the new fifth Anti-money laundering Directive. See references to international standards in COM (2016) 450, pages 3, 10, 13, 14.
1916 See particularly Chapter II above.

with the FATF's own recommendations.[1917] Non-conforming states can be put on a blacklist, with the consequence that conforming members will potentially exclude credit- and financial institutions from that state from participating in the international financial market place.

The FATF is comprised of 35 states, the Gulf Co-operation Council, and the European Commission. The 35 member jurisdictions include each of the EU-15 countries, as well as Iceland, Norway, Turkey and Switzerland. Europe is therefore the best-represented continent in the FATF, and is a significant help in propelling the efforts of the FATF. At the same time, however, those states just mentioned are also all bound by the ECHR and its protection of privacy and personal data, and the Commission is naturally invariably bound by the provisions of the Charter. Those human rights documents cannot be set aside by those states and the Commission in their role as member jurisdictions of the FATF.

The Anti-money laundering Directive is thus based on the recommendations of an international body, which bind the European Commission as well as 15 of the 27 European Member States individually. The consequence of the declaration of the incompatibility of the anti-money laundering measures with the principle of proportionality and the rights to privacy and data protection would therefore bring the Commission as well as the majority of the Member States into the uncomfortable situation of being bound by the FATF's standards, in which they have themselves taken "a pioneering role",[1918] and at the same time being prevented from implementing the standards set in the Recommendations because they conflict with the high standards of proportionality and human rights, which they have equally themselves helped develop.

This conflict makes the invalidation of the Anti-money laundering Directive a greater political conflict than the invalidation of the Data retention Directive. This political conflict should, however, be manageable. The fifteen Member States, the European Commission, and Iceland, Norway, and Switzerland make up together a block of 19 out of 37 members of the FATF. Bringing the FATF together to reverse the standards set wherever these standards violate human rights is thus uncomfortable and exceedingly embarrassing, but should not be an impossibility.

1917 See Chapter II above.
1918 European Economic and Social Committee, 13666/16, p. 3, 8.

In this context, the words of the ECtHR should be recalled to mind: "The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."[1919] The words of the ECtHR yet hold true and can easily be transferred to the context of anti-money laundering measures. In that case, the following principle should be applied: The actors pioneering in the use of new advanced measures to combat money laundering should also be pioneers in the assessment of the proportionality of these measures, and in the consistent protection of human rights.

The European Commission and the Member States concerned can therefore under no circumstances be permitted to argue in their defence the political obligation to implement standards set by an international organization[1920] of which they themselves make up the majority of members, and the standards of which they have actively helped to develop to the point where they clash with human rights.[1921]

## j. Epilogue: Alternative Transactions Systems

Instead of a conclusion, this chapter will end with an epilogue. It has now been established that the existing European anti-money laundering legislation is in conflict with the fundamental rights to privacy and data protection and should be invalidated upon a challenge of this legislation before the competent courts. However, no challenge is as yet pending with the CJEU, which is exclusively competent to pass judgment on the validity of any European directive. While a challenge may be made in the future, such a procedure is lengthy, and until the final judgment of the CJEU, the Directive remains valid and the disproportionate intrusions into the rights to privacy and data protection of the population remain a fact.[1922] A final question to be answered in the context of this thesis is therefore whether the use of alternative transactions systems may be an avenue to be taken



1919 ECtHR Case of *S and Marper v. United Kingdom* [2008], paragraph 112. See also Solove (2007), p. 411.
1920 See however COM (2016) 450 final, pp. 11, 14.
1921 See also Article 29 Working Party, Opinion 4/2014, p. 7.
1922 See in this context also Constant (2003), p. 481 f.

by persons wishing to properly protect their privacy and personal data against disproportionate intrusions.[1923]

**i. Virtual Currencies**

The problems the legislator is experiencing in the attempt to regulate virtual currencies have already been mentioned in Chapter IV above. The difficulty lies primarily in the fact that a virtual currency system is not an entity that can be fit into any of the categories of the Anti-money laundering Directive. It is rather a loose global network of individuals running the same code.[1924]

The network itself therefore eludes the categories of the Anti-money laundering Directive. Only businesses connected to the virtual currency environment and operating within the territory of the European Union can be covered by the Directive. This concerns primarily exchanges[1925] and other service providers, such as custodial wallet providers.[1926] These businesses are obliged entities under the Anti-money laundering Directive, and they therefore must comply with their identification, monitoring, reporting, and data retention obligations under the Directive.

Transactions, on the other hand, largely escape monitoring. To monitor transactions on the blockchain is not the responsibility of any obliged entity, unless one party to such a transaction is an obliged entity. This is the case where a user connects to an exchange, for instance. However, it is relatively simple to use virtual currencies without making use of the services of an obliged entity, in particular because service providers connecting to the virtual currency environment can be based anywhere in the world, including in countries where the anti-money laundering oversight is not quite as rigorous as in Europe.[1927]

In addition, there are a number of technologies that can be used to conceal one's identity when accessing the service, which range from using a different wallet address for each transaction, avoiding obliged entities and making use of mixers, concealing one's IP address, and using Tor hidden services. If such privacy enhancing technologies and tools are used properly and carefully, the user can

1923 Dowd (2014), p. 80; Marx (2003), p. 369 f.; Mezzana/Krlic (2013), p. 8 f.
1924 Hildner (2016), p. 488 f.
1925 Kaiser (2016a), p. 223 f.
1926 COM (2016) 450 final, p. 12 f.
1927 See in this context also Eymann/Utz/Süptitz (2013), p. 308 f.

achieve a high degree of privacy and anonymity in the sense of non-identifiability. In this way, virtual currencies may allow users with the necessary set of technical skills to achieve a degree of privacy online almost as high as is provided offline by cash. Just as there is no entity monitoring the blockchain, there is also no entity charged with monitoring all transactions of the population which are carried out using cash.[1928] Therefore, virtual currencies could be seen as a valuable tool for those users who wish to escape the rigorous surveillance mechanisms[1929] in place to monitor all channels of financial transactions other than cash.

However, there is a grave danger for a user's privacy connected to virtual currency systems, which is the blockchain itself. The blockchain is essentially a record of all transactions ever carried out through the system, which will remain accessible to anyone for the foreseeable future. Technology, and particularly cryptography, is subject to rapid change, however. The technologies used in order to conceal one's identity may not be effective for a long time, due to unforeseeable changes in the available technologies to counter the measures taken by the user. This danger becomes particularly apparent when one considers the long-term availability of data on the blockchain. The risks to a user's privacy while using virtual currencies are impossible to gauge properly ex ante.

What is clear, however, is that users must take additional measures to safeguard their privacy when using virtual currencies, as the omission of such additional measures makes virtual currencies a very unsafe system for the average user in terms of privacy and data protection. It has been shown that the great majority of regular users can be identified based on their behavioral patterns on the blockchain, and that even users with the necessary technical skill and motivation to hide their identities are rather easy to track.[1930] This ease in observing the user's transaction patterns and spending behavior is a great threat to the privacy of all users, which limits the use of virtual currencies for enhanced privacy.

Therefore, virtual currencies may potentially be used in order to escape the surveillance mechanisms of the anti-money laundering framework. However, the avoidance of surveillance according to the measures of the Anti-money laundering

1928 Kaiser (2016b), p. 32 f. See also Luther (2016), p. 402.
1929 Article 29 Working Party, Opinion 4/2014, p. 6; Murck (2013), p. 96; Mezzana/Krlic (2013), p. 8 f.
1930 Meiklejohn et al. (2016), p. 92.

Directive does not necessarily result in enhanced privacy. The open architecture of the blockchain should be regarded as a serious threat to the privacy of the majority of users, who must be very careful in their use of virtual currencies in order to avoid linking of their transaction history to their identities. The long-term impact of virtual currency systems on the privacy of users will be observed with interest in the coming years.

**ii. Informal Value Transfer Services**

Just like virtual currencies, informal value transfer services are not comprehensively covered by the Anti-money laundering Directive.[1931] Informal Value Transfer Services also to some extent escape the rigorous anti-money laundering regime, though in a different way than virtual currencies do. Hawaladars are obliged entities under the Directive and should therefore in principle comply with their obligations under the Anti-money laundering Directive, and many hawaladars do so.

However, a lot of hawaladars operate underground, out of sight of the authorities and without complying with their anti-money laundering obligations.[1932] When a hawaladar who operates underground carries out a transfer, it is likely that the hawaladar does not comply with his duties of identification, monitoring, reporting, and data retention. In fact, many unlicensed hawaladars actively avoid contact with law enforcement agencies in order to avoid penalties for the operation of an unlicensed financial transfer business.[1933] Therefore, it is very unlikely that a customer of a hawaladar will be confronted with the obligations arising out of the anti-money laundering legislation. The services of a hawaladar who operates underground could thus be used to avoid the surveillance introduced by the anti-money laundering legislation.

While the privacy of a hawaladar's customer is therefore rather safe from intrusions caused by anti-money laundering measures, there are different risks involved in using the services of a financial service provider who operates underground and does not comply with the different regulations in place to secure financial services. While not all users will be negatively affected by the lack of compliance

1931 See also Chapter IV above.
1932 Lascaux (2014), p. 94; Johnson (2011), p. 157.
1933 Redin/Calderón/Ferrero (2012), p. 19; Johnson (2011), p. 155.

with regulations concerning the financial services industry, the safeguards may be very useful for the protection of customers in the case that any of their interests are injured. The body of regulations that is to provide safety in such cases consists of, among other things, minimum capital requirements, oversight mechanisms, and obligations of disclosure, and non-compliance with these requirements can be punished with fines and in severe cases with imprisonment. Those obligations are generally avoided by hawaladars, which may be a disadvantage for some customers. On the other hand, hawaladars do secure their business transactions by vouchsafing for them with their personal reputation,[1934] which may be a preferable guarantee to other customers. It may be left up to the individual customer to make the choice whether he or she prefers the one type of security or the other, and whether he or she chooses to make use of the services of an unregistered hawaladar.

To sum up, both virtual currency systems and informal value transfer systems could be used in order to avoid the surveillance measures of the Anti-money laundering Directive. However, neither of the systems can be used for all of the financial services required by a user when that person is well-integrated in society. As has been shown earlier, it is nearly impossible to take part in society without using financial services for instance in order to receive wages and pay insurances and taxes: Neither a Hawala transaction nor virtual currencies are likely to be accepted in these cases at this point in time or in the foreseeable future. In addition, the use of these two systems is accompanied with another set of risks, such as the risks to privacy inherent in the use of virtual currencies, and the risks faced by the customers of hawaladars avoiding financial regulations. In sum, while it is possible to carry out individual transactions outside of the conventional banking system, the average European cannot avoid the services of obliged entities. Therefore, there is no viable alternative to the conventional banking sector that might offer enhanced protection of privacy and personal data, which adds to the urgency with which the disproportionality of the Anti-money laundering Directive must be addressed.



1934 Redin/Calderón/Ferrero (2012), p. 13; Razavi (2005), p. 285; Razavy/Haggerty (2009), p. 146 f.

# Chapter X

## A Way Forward

## Outline:

a. Introduction
b. The Essence of Privacy
    i. Case Law
    ii. Proportionality vs. Essence
c. Die Wesensgehaltsgarantie
    i. The Guarantee
    ii. The Guarantee and Proportionality
    iii. Result: Human Dignity Forming the Essence of the Right to Privacy
d. A Holistic Approach
    i. Protecting the Essence of Privacy
    ii. A Fragmented Approach
    iii. Die Überwachungsgesamtrechnung
    iv. Privacy and Dignity
    v. A Holistic Approach
    vi. Applying a Holistic Approach
    vii. Constitutional Identity
e. Conclusion

## a. Introduction

In the previous chapter, it has been argued that the rights to privacy and data protection are disproportionately limited by the measures of the Anti-money laundering Directive. According to the assessment made in this thesis, the Directive would have to be invalidated by the CJEU if it was ever challenged before the Court. However, this thesis is only concerned with one directive, while there are numerous other legal acts which might warrant a similar assessment. Indeed, laws containing legal bases or legal obligations for data processing are passed at a furious rate, and much faster than they can be assessed, and perhaps challenged. Some of the data processing operations may be perfectly in accord with the principle of proportionality. Some are not, as the example of the Anti-money laundering Directive shows.

Due to the large number of processing operations, it becomes more difficult to apply the proportionality test. It is the sheer volume of data processing operations on which an assessment should focus; this volume pushes the proportionality of individual legal measures into the background. Indeed, it may be questioned whether it is sustainable to rely on a system in which legal measures must be challenged individually in a lengthy and costly legal procedure, particularly if it is recalled to mind that for any measure which is successfully challenged, a multitude of new measures are introduced.[1935] It would appear that the magnitude of legal measures intruding into the individual's privacy cannot be overcome with the traditional tools of the principle of proportionality. The protection granted by the principle of proportionality simply does not reach far enough to comprehensively protect the privacy of individuals. It is therefore necessary to develop a more suitable mechanism for the protection of the privacy of individuals.

The assessment of the proportionality of interferences with the rights to privacy and data protection caused by European legal acts is based primarily on article 52 of the Charter. This article also contains the condition that interferences with the rights contained in the Charter must not go so far as to adversely affect the essence of the right. As the CJEU has yet to define the term "essence", the discussion of



1935 See for instance this list of surveillance measures introduced in recent years https://digitalcourage.de/blog/2016/materialsammlung-ueberwachungsgesamtrechnung#staat (last accessed 3 January, 2018).

this point is particularly difficult. The CJEU has so far usually only stated in case law that certain disputed measures did or did not "adversely affect the essence of those rights".[1936] The intention of this chapter is not to anticipate such a definition, but to outline a potentially viable approach to the protection of the essence of the right to privacy.

The essence of the right to privacy also plays a role in the data retention case law on both the European and the national level. While the CJEU mentions the essence of the right to privacy only in order to state that it is not affected,[1937] the BVerfG in its decision makes some interesting observations in that direction. The BVerfG demands of the lawmaker to protect the privacy of the public by not only considering the legality of individual measures of surveillance, but by surveying the entire landscape[1938] of surveillance measures already in existence before considering the addition of further measures.[1939] The term 'landscape' in this context was chosen for this thesis because it expresses that the different surveillance measures affecting the different areas of an individual's private life must be mapped out to assess the concentration and severity of these measures. The connection to European law is made by the BVerfG itself, by pledging the representatives of the Federal Republic to promote a restriction of mass surveillance also on the European level, and warns the lawmaker that it cannot simply route legal obligations to introduce measures of mass surveillance through the European lawmaker.[1940]

This approach proposed by the German Constitutional Court may be described as holistic. It is to be introduced in this chapter in detail, and an attempt will be made to translate it to the European level. It should be noted at the outset, however, that this chapter can only present a short overview of this complex and a beginning of a discussion in this regard. A more thorough analysis of this issue would demand the research and draft of a second, separate thesis and dissertation.

1936 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 39.
1937 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 39.
1938 See in this context also *Gellert's* comments on the connection between data protection, privacy, and environmental protection: Gellert (2015), p. 11 f.
1939 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Gietl (2010), p. 403.
1940 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Gerven (1999), p. 44 f.

This chapter will begin with a discussion of the content of the essence of the right to privacy (b) and the Wesensgehaltsgarantie (c). In section (d), the holistic approach as outlined by the BVerfG will be introduced and translated to the European level.

## b. The Essence of Privacy

Limitations of fundamental rights protected by the Charter must comply with the conditions of Article 52 of the Charter.[1941] Article 52 (1) of the Charter reads as follows:

> "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

The conditions enumerated in article 52 of the Charter are primarily a codification of the case law of the CJEU, which in its decisions has been referring to these conditions, among them consistently to the essence of fundamental rights.[1942] However, the definition of the essence of the right to privacy, or of any other rights mentioned in the Charter, has not yet been discussed in detail by the Court.

### i. Case Law

In most of the CJEU's case law, the Court has limited its assessment of the essence of the right in question to the simple statement that the essence of the right was not affected by the measure in question. When assessing the interference with the right to privacy enshrined in article 7 of the Charter in the *Digital Rights Ireland* case, the Court states that although the retention of data as set out in the Data retention Directive "constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from article 1 (2) of the directive, the directive does not permit the acquisition of



1941 These conditions have already been discussed in detail in Chapters V and VIII above.
1942 See for instance CJEU Joined Cases C-293/12 and C-594/12, Digital Rights Ireland [2014], paragraph 38; CJEU Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2016], paragraph 94; CJEU Case C-362/14 Schrems [2015], paragraph 94.

knowledge of the content of the electronic communications as such."[1943] The Court omits a detailed discussion in this context of the extensive conclusions which can be drawn from the metadata on the content of the communications, which would put the statement that the Directive does not permit the acquisition of knowledge of the content of the communications into perspective.

However, the Court's reference to the fact that the existing interference with the right to privacy and data protection is not as severe as it would be if the content of the communications were revealed, cannot be taken to mean that the essence of a right cannot be affected by a certain interference as long as an even more serious interference is thinkable. The fact that the Court held that the essence of the right to privacy was not triggered by the collection of metadata in this case does not mean that no interference short of the complete debasement of a right can affect the essence of that right.

The CJEU does come back to this issue in its later *Tele2 Sverige* judgment and acknowledges the fact that the data collected "provides the means […] of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."[1944] Unfortunately, the Court then fails to consider this interference as no less serious as if it did reveal the content of the communications.[1945] The Court specifically relates the possibility of knowing the content of communications and the possibility of accurately inferring the content of communications based on metadata, and explicitly states that it regards one as no less sensitive than the other, only to finally decide not to treat those equally sensitive categories of information as equally serious. Naturally, the existing metadata have to be aggregated into a personality profile first.[1946] This aggregation is, however, very simple, due to their typically clear structures of metadata. These structures also may in fact yield information about a conversation more readily than the conversation itself, as conversations can take numerous different shapes, while metadata is usually more easily readable.[1947] However, the relatively simple means of doing so, as well as the fact that such

1943 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 39.
1944 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 99.
1945 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 101. See also Petri (2008b), p. 730.
1946 See also Article 29 Working Party, Opinion 4/2014, p. 4; Korff (2014), p. 115; Hensel (2009), p. 529.
1947 Article 29 Working Party, Opinion 4/2014, p. 5. See also Korff (2014), p. 85 f.; Petri (2008b), p. 730 f.

profiles are being established by many data processors already, would have made explicit protection of the as yet unassembled metadata highly desirable. As this decision is not further explained or substantiated by the Court, the reasoning behind this unequal treatment is incomprehensible.[1948]

To return to the *Digital Rights Ireland* decision, the Court there goes on to examine the interference of the measures with the essence of the right to data protection in article 8 of the Charter, and comes to the conclusion that this is also not an interference of sufficient magnitude to adversely affect the essence of this right, because

> "certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of data."[1949]

The Court leaves open whether such very basic principles and safeguards are sufficient to avoid an adverse impact on the essence of the right to data protection, or if the protection of the essence of this right goes further than mere data security.

Only seldomly did the CJEU find the essence of a right adversely affected. In *Digital Rights Ireland*, the Court decided that the collection of metadata about communications as provided by the measures of the Data retention Directive was a particularly serious interference, but not of such a character as to adversely affect the essence of the right to data protection and privacy, as the content of the communications was not revealed. However, in its 2015 judgment in the case *Schrems,*[1950] the Court had the opportunity to develop this line of case law further, as the measures in question in that judgment did reveal the content of communications. In this case, the Court stated that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental



1948 Kunnert (2014), p. 775.
1949 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 40. See also Grimm/Bräunlich (2015), p. 290 ff. for further background on data security issues.
1950 CJEU Case C-362/14 *Schrems* [2015].

right to respect for private life, as guaranteed by Article 7 of the Charter".[1951] However, as in all previous judgements in which the CJEU mentioned the point of the essence of a right, a detailed discussion of this point is conspicuously missing. Therefore, the CJEU's judgment in *Schrems* unfortunately allows for few positive conclusions concerning the concept of the essence of privacy beyond the fact that the contents of communications are certainly protected by this notion. Therefore, the essence of the right to privacy is one concept on which there is singularly little reliable information. The lack of a definition is at odds with the position of the essence as one of the conditions for the legality of interferences.

Based on the foregoing, it can therefore be stated that the essence of a fundamental right is a concept not conclusively defined in case law. The CJEU always refers to the essence of a fundamental right in its assessment of a measure, but it seldomly adds further explanation to fill this term with life. One of the few cases in which the Court held that the essence of a right was negatively affected is *Schrems*, in which the Court invalidated an agreement due to the tangible possibility, that third parties would lean the contents of communications of data subjects. Beyond the fact that the contents of communications are therefore protected as essential, there are so far few clues pointing to what the essence of a right is. In particular, the Court has not developed a test, with which it may assess whether the essence of a right is affected. Such a test only exists for the principle of proportionality so far.

**ii. Proportionality vs. Essence**

The Court thus generally limits itself to a very short and not particularly meaningful discussion of the essence of the rights in question. The scant attention which the Court appears to grant to the discussion of the essence of privacy in its judgments leads to the question of its overall significance in an assessment of the compatibility of a certain measure with human rights.

The elaborate case law on proportionality is seen by some writers as a sufficient guarantee against overreaching measures, as no interference can be proportional and at the same time affect the essence of the right to privacy.[1952] The question whether a measure encroaches upon the essence of a right would thus always end with the proportionality assessment, as a measure which is deemed proportional

1951 CJEU Case C-362/14 *Schrems* [2015], paragraph 94.
1952 Trstenjak/Beysen (2012), p. 280; Gerven (1999), p. 44 f. See also Chapter VIII above.

cannot infringe upon the essence of a right; when a measure is deemed disproportional, the measure will already be invalidated for that reason, making a discussion of the essence of privacy in that context irrelevant. In fact, the only divergence between the concepts of the essence of a right and the proportionality of a measure would be possible in such cases as in that of the Data retention Directive, where the measure is held to be disproportionate to the aim pursued, but not to affect the essence of the right. Proportionality will therefore usually offer a higher protection of an individual's rights than the protection of the essence of that right, as the threshold for disproportionality of a measure is lower than that for affecting the essence of a right.

This line of argumentation has some merit. It is true that it is unlikely that any measure could be held to be proportionate to the aim pursued, but at the same time to interfere so radically with the right in question that its essence is affected. The CJEU's own case law argues for both positions. The CJEU itself has developed the point of the essence of a right in its case law early on and consistently referred to that formula. The formula in article 52 of the Charter is a codification of the settled case law[1953] of the Court.[1954]

On the one hand, the Court concentrates on the proportionality assessment in most of its case law on human rights infringements.[1955] The assessment of the respect of the principle of proportionality usually determines the Court's assessment of the legality of a measure. Advocate General *Tizzano*'s symptomatic statement in case C-453/03 *ABNA* may serve as an illustration of the preference for a proportionality assessment:

> "The central ground alleging invalidity in the present case is unquestionably that relating to proportionality. This is all the more true in view of the fact that the relevant case-law does not only, as has been seen, cover in part the ground relating to the legal basis but also, as can be clearly seen in the present context, is superimposed on the review of the compliance with the fundamental rights of property and freedom to



1953 See for instance CJEU Joined Cases C-293/12 and C-594/12, Digital Rights Ireland [2014], paragraph 38; CJEU Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2016], paragraph 94.
1954 Wehlau/Lutzhöft (2012), p. 49.
1955 Wehlau/Lutzhöft (2012), p. 46.

> carry on a trade or profession, thereby rendering a specific analysis of that review unnecessary."[1956]

On the other hand, however, the Court generally mentions the essence of the right in question before moving on to the proportionality assessment. In the *Digital Rights Ireland* case, for instance, the Court first establishes the interference of the measures in the Data retention Directive with the rights to privacy and data protection, and then discusses the question whether the essence of the rights to privacy and data protection is adversely affected by these measures.[1957] Only after negating this question does it move on to a proportionality assessment. It is difficult to make statements on what the Court does when it does find the essence of a right adversely affected, as there are so few examples of this happening, and only one in the context of the right to privacy and the protection of personal data. In *Schrems*, the Court did not discuss the proportionality of the measures in question, but invalidated the directive based on the negative effect of the measures on the essence of the rights to privacy and data protection.[1958]

Additionally, the provision of article 52 of the Charter itself makes it very clear that the essence of a right and the proportionality of a measure are two very different things which must be accommodated individually. A systematic assessment of article 52 of the Charter shows that its first paragraph is concerned with the principles of legality and the protection of the essence of the rights. Only the second sentence is dedicated to the proportionality principle. Clearly, the two notions of proportionality and essence of a right could have been connected into one concept if the nexus had been closer, but instead, the two elements were drafted as two separate concepts and kept separate over an extensive set of case law.

Therefore, the notion that the essence of a right has no independent meaning due to its close connection to the principle of proportionality cannot convince. On the contrary, prominent legal scientists are of the opinion that the protection of a human right must be treated with special care, and should not be simply one

1956 Opinion of *Advocate General Tizzano* in CJEU Joined Cases C-453/03, C-11/04, C-12/04 and C-194/04, *ABNA and others* [2005], paragraph 74.
1957 CJEU Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* [2014], paragraph 39, 40.
1958 CJEU Case C-362/14 *Schrems* [2015], paragraph 94. The Court would no doubt also have invalidated the directive based on lack of respect fort he principle of proportionality, but it omitted a discussion of this point.

interest of many which are taken into account in the proportionality test.[1959] Those scholars consequently demand of the CJEU to develop the essence of a human right into a fully-fledged substantial guarantee.[1960] This view is correct and is endorsed in this thesis, but it is a claim thus far not heard by the Court.

## c. Die Wesensgehaltsgarantie

### i. The Guarantee

Searching for this independent meaning of the protection of the essence of a right on a European level is, due to the meagre case law on the topic so far and lack of other authoritative sources, not a very fruitful undertaking. A step back to Member State level could, however, bring some life to the concept of the essence of rights. Naturally, the CJEU is bound solely by the text of the Charter when interpreting the term essence in its case law and does not take human rights guarantees on Member State level into account. But the Court itself has frequently stated that the Member States' constitutional traditions of human rights as well as international treaties significantly shape the development of human rights on Union level.[1961] In the CJEU's own words, "the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories."[1962] This approach is also codified in article 6 (3) TEU which reads, "Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law."

In this context, a look into the German Constitution may prove helpful in shaping a concept of the essence of a right.[1963] The German Constitution (*Grundgesetz*, *GG*)



1959 Wehlau/Lutzhöft (2012), p. 50.
1960 *Von Danwitz*, quoted in Wehlau/Lutzhöft (2012), p. 50. See also Manger-Nestler/Noack (2013), p. 505.
1961 Möllers/Redcay (2013), p. 411; Barak (2013), p. 182 f.; Kahler (2008), p. 451.
1962 CJEU Opinion 2/94 *Adhésion de la Communauté à la CEDH* [1996], paragraph 33. See also CJEU Opinion 2/13 *Adhésion de l'Union à la CEDH* [2014], paragraph 37; Manger-Nestler/Noack (2013), p. 505.
1963 See also Craig/De Búrca (2015), p. 551 for a similar comparison in the field of proportionality.

contains in article 19 (2) GG a clause that is strikingly similar to that in article 52 (1) of the Charter. Article 19 (2) GG provides that "Fundamental rights may under no circumstances be touched in their essential content."[1964] The close connection of the wording of the two provisions makes the abundant case law and theoretical discourse in literature a potentially great help in the search for the meaning of the concept of the essence of a right as mentioned in the Charter.

Article 19 (2) GG is known as the *Wesensgehaltsgarantie*, an essentially untranslatable term, which, for the purposes of this discussion, could be translated with the term "guarantee of the preservation of the core values of a human right". A perhaps better translation would use the term 'essence' which will be avoided here to avoid confusion with the concept of article 52 of the Charter. In the following sections, the terms 'core' or 'core values' will be used when referring to article 19 GG, and regarding the concept of the '*Wesensgehaltsgarantie*', the original German term will be used, or it will be abbreviated by calling it simply 'the guarantee'.[1965]

The point that makes the German doctrine so interesting and potentially valuable in the search for the meaning of the term 'essence' in article 52 of the Charter is the fact that the *Wesensgehaltsgarantie* in the German constitution is the starting point for the development of such a point in many other constitutional systems, such as in France and Italy,[1966] and has since then become a basic theory of European constitutional legal theory and tradition.[1967] Therefore, as the Court considers itself guided by Member States' common constitutional traditions, a search for a substantive content for the term 'essence' in article 52 of the Charter would necessarily lead it to the *Wesensgehaltsgarantie*.[1968] Indeed, it is not unlikely that the CJEU was guided by this concept when developing the conditions for the legality of interferences with human rights in its own case law.

What the term 'core value' is to mean precisely is not much easier to determine than the meaning of the term 'essence'. Naturally, each human right has gone through rapid developments in the past decades. This is particularly true for the rights

1964 The original German wording of article 19 (2) GG is "In keinem Falle darf ein Grundrecht in seinem Wesensgehalt angetastet werden." See also Puschke/Singelnstein (2005), p. 3536.
1965 The term guarantee is particularly fitting, as the text of the provision does not allow for exceptions. See below.
1966 Wehlau/Lutzhöft (2012), p. 49 f.
1967 Wehlau/Lutzhöft (2012), p. 49; Möllers/Redcay (2013), p. 411.
1968 See also Barak (2013), p. 182 f.

to privacy and data protection. In addition, the core, or the essence, of a right is of course always dependent on the personal point of view of an individual, and those points of view have a tendency to develop rapidly, alongside major societal upheavals in the recent decades.[1969] Not surprisingly, lively discussions on the core values or the essence of rights have been led in the legal literature in Germany and elsewhere, and unlike the self-referential style of the CJEU, the BVerfG frequently references such scholarly discussions and opinions in its judgments. Therefore, the decades since the establishment of the German constitution have brought forth some interesting insights on this term.

The undisputed core of the principle is that article 19 (2) of the German Constitution protects and fences off a core content of each fundamental right, which is not subject to the disposal of the lawmaker.[1970] Thereby, article 19 (2) GG interferes in the balance between the constitution and the lawmaker.[1971] The lawmaker finds himself in the same difficult position as in the case of a proportionality assessment, being on the one hand bound to the constitutionally guaranteed human rights, but at the same time being permitted by the constitution to introduce limitations to those rights. At the same time, the lawmaker assesses the proportionality and legality of its own laws. The lawmaker must thus be restricted in his power to restrict fundamental rights. Alongside with the other limits introduced in article 19 GG, the guarantee tips the balance in favour of human rights.[1972]

The formulation "under no circumstances" furthermore appears to go farther than the protection of the essence of a right in article 52 of the Charter. The Charter speaks rather of 'respect', which is arguably a somewhat more amenable formulation. The very clear and explicit formulation of the guarantee in the German constitution is understood to bar all exceptions to the guarantee, and to bind not only the lawmaker, but all branches of government.[1973] The reason for such an absolute protection lies in particular in the connection of each human right to the inalienable right to human



1969 In particular the rights to privacy and non-discrimination have undergone major developments in recent years.
1970 Dix/Petri (2009), p. 533.
1971 *Remmert* in Maunz/Dürig, GG Art. 19 Abs. 2, Rn. 18.
1972 *Remmert* in Maunz/Dürig, GG Art. 19 Abs. 2, Rn. 18.
1973 *Remmert* in Maunz/Dürig, GG Art. 19 Abs. 2, Rn. 27.

dignity.[1974] Whenever the element of human dignity in a human right is infringed upon, the core values are infringed, and article 19 (2) GG is engaged.[1975]

The more amenable European formulation of 'respect' cannot, however, be construed to mean a weak protection of the essence of a right. The Court's case law clearly shows that the CJEU is awarding high protection to the essence of the right to privacy. This has become evident for instance in *Schrems*, where the Court found clear words to condemn a measure infringing upon the essence of the right to privacy.[1976]

**ii. The Guarantee and Proportionality**

Just like in European law, one of the other limits to interferences with human rights that stand alongside the guarantee is the proportionality principle.[1977] The discussion whether the core values of a right are already sufficiently protected by the principle of proportionality is not led to the same extent as on the European level, however. The BVerfG has made it abundantly clear in past decisions that the two concepts of *Wesensgehaltsgarantie* and the proportionality principle are two different concepts, which must be kept separate.[1978]

What precisely is the core of the right that is guaranteed by article 19 (2) GG is difficult to determine. In this way, there is another parallel between the core values of German constitutional law and the Charter on European level. Naturally, the vast differences between the rights contained in the constitution does not allow for one static formula, by which the core of a right must be measured. The BVerfG's ample case law does contain some indications. The Court has had the opportunity to refer to the core of the personality right, which includes the rights to privacy and data protection.[1979] In one particularly important decision, the so-called '*Diary Decision*', the BVerfG has found clear words to underline the importance

1974 BVerfG, 2 BvR 219/08 [2008], paragraph 17. See also Cannataci (2008), p. 4; Schröder (2016), p. 648; Bloustein (1984), p. 186 f.;

1975 *Remmert* in Maunz/Dürig, GG Art. 19 Abs. 2, Rn. 44.

1976 CJEU Case C-362/14 *Schrems* [2015], paragraph 94.

1977 The proportionality principle is an unwritten principle of constitutional law. It flows forth from the principle of legality in article 20 (3) GG. See *Grzeszick* in Maunz/Dürig, GG Art. 20, Rn. 107 ff.; Puschke/Singelnstein (2005), p. 3537.

1978 See for example BVerfG, 2 BvR 2029/01 [2004], paragraph 96; BVerfG, 1 BvR 2378/98 [2004], paragraph 112.

1979 According to the famous Census Decision, BVerfG, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 [1983]. See also Puschke/Singelnstein (2005), p. 3536; Lynskey (2014), p. 590 f.

of the protection of the core values of a right.[1980] The Court clarifies that even fundamentally important interests of the public cannot justify an intrusion into the core of this right; a balancing of interest does not take place.[1981] The Court here shows that the protection of the core values of the right to privacy to some extent coincides with the protection of a data subject's intimate sphere.[1982]

As has already been emphasised in Chapter V above, the right to privacy is particularly closely connected to the right to human dignity.[1983] This connection makes the strict protection of the core of this right so essential. This close connection between the core of the right to privacy and human dignity is also the reason why a balancing of interests in principle does not take place when the protected intimate sphere is concerned.[1984]

The protection of human dignity is absolute, as shown by Article 1 (1) GG, which states that human dignity is untouchable ('*unantastbar*').[1985] The German term is often translated with the term 'inviolable', but this term is not entirely correct. The German constitution protects a number of rights as '*unverletzlich*' (inviolable)[1986] but only one, namely human dignity, as '*unantastbar*' (untouchable). There is thus a marked difference in terms. This difference is also reflected by the BVerfG's treatment of human dignity compared to other rights. According to the case law of the BVerfG, human dignity cannot be limited in the same way as other rights: When human dignity is at stake, the interests of other parties are not considered; the principle of proportionality is not applicable, a balancing of interests does not take place.[1987] The rights which are considered 'inviolable' by the Constitution are not protected in as clear terms. They are subject to a proportionality assessment.

1980 BVerfG, 2 BvR 219/08 [2008], paragraph 17.
1981 BVerfG, 2 BvR 219/08 [2008], paragraph 17. See also Cannataci (2008), p. 4.
1982 This is explained in detail above in Chapter V. See also Maras (2012), p. 77.
1983 Martini (2009), p. 844; Linke (2016), p. 891; Schertz (2013), p. 723. See also Gurlit (2010), p. 1039; Baum (2013), p. 584.
1984 Martini (2009), p. 844; Linke (2016), p. 891; Schertz (2013), p. 723. See also Gurlit (2010), p. 1039; Cupa (2012), p. 425 f.
1985 See also Schertz (2013), p. 722. For an international view, see Lynskey (2014), p. 572.
1986 For instance the right to personal freedom (article 3 (2) 2nd sentence GG), the freedoms of creed, conscience, and religious or philosophical beliefs (article 4 (1) GG), the secrecy of communications (article 10 (1) GG) and the home (article 13 (1) GG) are all protected as 'inviolable'.
1987 BVerfG, 2 BvR 219/08 [2008], paragraph 17.

Article 1 (1) of the Charter protects human dignity as inviolable. However, human dignity is the only value protected in such terms in the Charter. This therefore places human dignity in the same singular position it holds in the system of the German constitution. The singularity of the term is the crux of the formulation: It shows the paramount importance of the right to human dignity in both systems. Therefore, the protection of human dignity must be as near to absolute as possible, and a proportionality assessment as in the application of other rights cannot take place.

The BVerfG has furthermore clarified that the core values of each human right must be determined individually, as they are shaped and developed in such different ways. The unalienable core of a human right must therefore be determined for each individual human right, depending on its particular importance in the general system of human rights.[1988] This is another parallel between the European concept of the essence of a right and the German concept of core values. In addition, many human rights are not clearly defined and applied to specific instances, but protect a number of different values in different ways, the protection of which furthermore being prone to change over time. The complex of personality rights protected under German constitutional law is a prime example, as it protects within one provision among other values the rights to privacy and data protection, which each have their own core values, and which are not comparable to one another, or to the other personality rights protected alongside them.[1989]

In conclusion, it can be said that the core values of a human right are such elements which are responsible for the retention of a meaningful identity of that right, in the face of possible legal restrictions of the right by the lawmaker and the executive.[1990] All other clarifications beyond this core definition depend on the right and on the infringement in question.

### iii. Result: Human Dignity Forming the Essence of the Right to Privacy

The excursion into German constitutional law served to show the close connection between the right to privacy and human dignity. While the German Constitutional Court has not yet defined a universal definition for the concept of the core values

1988 See BVerfG, 2 BvR 2029/01 [2004], paragraph 96. See also Gurlit (2010), p. 1036.
1989 *Remmert* in Maunz/Dürig, GG Art. 19 Abs. 2, Rn. 40. See also Lynskey (2014), p. 590 f.
1990 *Remmert* in Maunz/Dürig, GG Art. 19 Abs. 2, Rn. 41.

of a right, it has had the opportunity to emphasise the close connection between the privacy of individuals and human dignity.[1991] This connection is evident in, for instance, the remarks made on the protection of the intimate sphere of an individual's privacy.[1992] According to the BVerfG's settled case law, the intimate sphere of an individual's privacy must be protected as strictly as possible, a consideration of the interests of others does not take place.[1993]

One may therefore go so far as to say that the intimate sphere of an individual's privacy is inviolable. Such inviolability is based on the connection between the aspects of privacy falling into the intimate sphere and human dignity. However, the intimate sphere also marks the centre of an individual's privacy. It may therefore be considered that those aspects of privacy which fall into the intimate sphere are also protected as the core values of the right to privacy. The intimate sphere of privacy therefore may be considered to mark the minimum of aspects protected as core values. It should be considered a minimum because the protection of core values may extend beyond the intimate sphere: It is not unlikely that some aspects falling into an individual's private sphere fall into the protection of the core values, but it is very unlikely that the protection of core values is narrower than the intimate sphere.

The CJEU has not yet developed its stance on the content of the essence of a right, or on the connection between the right to privacy and human dignity. However, although these things have not yet been discussed and stated explicitly by the Court, the situation on the European level is so similar to that of German constitutional law that it may be expected that the CJEU would define the essence of a right along similar lines. Human dignity takes up a singular position in the European legal system: it is the only right protected as "inviolable" in the Charter. If this inviolability of human dignity is to be meaningfully protected, it must also protect those aspects of the right to privacy which are connected to human dignity. This interpretation is also in line with the existing case law of the CJEU. For instance in *Schrems*, the CJEU stated that the protection of the content of communications is covered by the essence of the right to privacy.[1994] The content of communications will often be connected to aspects of the intimate sphere of an individual. Again,



1991 See BVerfG, 2 BvR 219/08 [2008], paragraph 17.
1992 The theory of spheres was introduced and discussed in Chapter V section (d) above.
1993 Martini (2009), p. 844; Linke (2016), p. 891; Schertz (2013), p. 723.
1994 CJEU Case C-362/14 Schrems [2015], paragraph 94.

these aspects of the right to privacy which are connected to human dignity should be protected as essential, but the protection of the essence of a right may well extend beyond these aspects.

For the purpose of this thesis, therefore, the essence of the right to privacy will be considered to consist at least of those aspects of that right which are connected to human dignity. After thus establishing a content for the term 'essence', the question to be discussed in the following section is whether the essence of the right to privacy is properly protected.

## d. A Holistic Approach

### i. Protecting the Essence of Privacy

Based on the explanations given above, it can be said that in principle, the standards applied by the CJEU and the BVerfG to the protection of essential core values of a right are very similar. Both attach a number of conditions to interferences with a human right by the lawmaker, among which are the principles of proportionality, and the protection of the essence or core values of a right. The content of the terms essence and core value are moreover very similar, though it appears that the German constitutional system so far places more weight on the elaboration of this concept than its European counterpart.

The protection of the essence of a right is a strong safeguard, but it may not be sufficient to guard properly against all possible infringements.[1995] The weakness of both systems is that each of them are limited to examining one law at a time, to which the parameters of proportionality and protection of the essence or core values are applied. This weakens the protection of this provision, as particularly the rights to data protection and privacy are assaulted by an unprecedented number of infringements. This concerns especially the increasing number of measures of mass surveillance with which each data subject is confronted, the lack of transparency and accountability in the collection and processing of personal data by both private and public actors nationally and internationally, and the (resulting) lack of meaningful tools at the disposal of data subjects for the protection of their personal data and privacy. The high number of interferences and their combined

1995 Article 29 Working Party, Opinion 1/2014, p. 21 f.

effect on the privacy of individuals cannot be kept in check with the traditional defences at the disposal of data subjects.

This in turn creates the difficulty that the combination of the number of infringements very easily can affect the essence or core values of a right. However, the Courts are, under the tests presently applied, bound to examine each piece of legislation in isolation and only upon a challenge, disregarding the possible aggravating factors created by the surrounding legal and factual situation. It was therefore an almost revolutionary move of the BVerfG when it took the first step to developing a new approach, which may perhaps lead to the development of a holistic view of surveillance.

**ii. A Fragmented Approach**

Under European law, whenever a certain measure is challenged before the CJEU, this piece of law is examined in isolation without considering other legislation not included in the challenge. If the legality of a certain measure is disputed, that measure is examined until the CJEU is satisfied that the measure does or does not fulfil the requirements of the Charter, particularly the principle of proportionality. This means, in turn, that no single directive or regulation can introduce measures which go so far as to be incompatible with these conditions. Therefore, were the legislator to introduce a hypothetical single regulation or directive compelling all private institutions to allow law enforcement direct access to all of their data for the purpose of combating crime in general, it would be destined to be invalidated upon a challenge before the CJEU.

The Data retention Directive may serve as a good example in this context. The Data retention Directive did not go quite so far as that, but its measures were rather comprehensive in scope.[1996] It concerned data collected by internet and telecommunications services providers, and stipulated the retention of this data by the providers as well as access to these databases by law enforcement agencies. In comparison with the Anti-Money Laundering Directive, the Data retention Directive was significantly different in two ways. In the first place, the Directive did not define specific crimes for which the data collected by the service providers could be accessed by law enforcement. Instead, it only referred to 'serious crime' in a general way, and allowed each Member States to define which crimes would

1996 See also Brunst (2011), p. 619.

be categorized as serious (article 1 DRD).[1997] As has been shown in Chapter IX, the Anti-money laundering Directive is ostensibly clearly limited to the crimes of money laundering and terrorist financing, although it is in the nature of money laundering to be connected to another crime as predicate offence, and it is equally in the nature of terrorist financing to be connected to further crimes of a terrorist nature. Predicate offences to money laundering are still left to some extent to the Member States to define, the wide extent of which has already been discussed and criticised in detail above. In the second place, the Data retention Directive allowed law enforcement agencies access to the databases compiled by the services providers directly, whereas the Anti-Money laundering Directive introduces primarily a push-system, in which the service provider sifts through transaction data to filter out suspicious transactions, and passes only those on to the Financial Intelligence Units. However, as has been shown in the previous chapter, it appears that the lawmaker is unable to resist the temptation of allowing FIUs more access, and the pull-system is slowly gaining in importance.[1998]

The Data retention Directive was held by the CJEU to be in violation of article 7 of the Charter of Fundamental Rights. The CJEU criticized particularly the comprehensive nature of the data collection. The Court said, specifically, that

> "national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy".[1999]

1997 See also the first concern discussed in Chapter IX.
1998 See also the ninth concern discussed in Chapter IX above.
1999 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 105.

The Court continues to deplore that

> "Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime".[2000]

This extensive scope and the lack of exceptions is the basis on which the Court deemed the data retention regime disproportionate. The Court therefore found that the interferences authorised by this particular piece of legislation were too extensive in scope.

However, it must be emphasised that this finding only concerns the far-reaching measures contained in the Data retention Directive. Nothing in the existing test applied by the CJEU can prevent the lawmaker from creating surveillance of the same scope as was found disproportionate in the Data retention Directive, if only the lawmaker cleverly divides the measures up into different pieces of law. As those different pieces of law would have to be examined in isolation, the intrusion into the right to privacy caused by each individual law may well be found to be proportionate, although they would be deemed disproportionate if viewed in combination. To repeat a statement by *Simitis* made back in 1998, "the vulnerability of the individual is exponentiating; the defence instruments are blunting."[2001]

This statement of *Simitis* neatly summarises the difficulty posed by the fragmented approach. For instance, it was argued in this thesis that the Anti-money laundering Directive is disproportionate. On the basis of the CJEU's existing case law, it may be expected that the CJEU may share this opinion if a challenge were to bring the Directive before the Court. The situation would, however, be different if the lawmaker were to split the measures of the Anti-money laundering Directive into, for instance, four directives. Each of the four measures of the anti-money laundering approach may be regulated in one directive: identification of customers



2000 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 106.
2001 Simitis (1998), p. 2477; Boehme-Neßler (2016b), p. 422 repeats this sentiment in the context of Big Data.

of the financial sector, monitoring of transactions, reporting of suspicious activity, and retention of data. In such a case, it could not be stated with equal confidence that the Court would adopt the opinion that each of the individual directives interferes disproportionately with the rights to privacy and data protection. This is due to the examination of measures in isolation, although the combined effect of measures remains the same.

In this context, it should be mentioned that such fragmentation of laws is already routinely practiced by the lawmaker both on both European and national level, although one might not wish to go so far as to accuse the lawmaker of intentionally circumventing the protection of the essence of a right. However, regardless of the underlying intention, serious interferences with fundamental rights are the consequence of the combination of these provisions. A good example of such fragmentation of the law has only recently been provided by the European lawmaker. In December 2016, the European lawmaker passed an amendment[2002] to Directive 2011/16/EU[2003] on administrative cooperation in the field of taxation, according to which tax authorities are to be granted, among other things, access to all customer due diligence information collected by obliged entities under the provisions of the Anti-money laundering Directive.[2004] Without assessing the details of this access right in more depth at this juncture, it is clear that such access by tax authorities is an interference with the rights to privacy and data protection of the data subject, and that the provisions of this Directive are intimately connected with those of the Anti-money laundering Directive. Instead, they are contained in two separate pieces of legislation. They would therefore have to be challenged individually, and their proportionality would be examined in isolation. The Directive on administrative cooperation in the field of taxation may therefore serve as a clear illustration of the threat outlined above.[2005]

2002 Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, OJ L 342, 16.12.2016, p. 1–3.
2003 Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, OJ L 64, 11.3.2011, p. 1–12.
2004 See the fifteenth concern discussed in Chapter IX above. See also Kaetzler (2008), p. 180; Lennon/Walker (2009), p. 40; Beckmann (2017), p. 974 f.
2005 See also Hamacher (2006), p. 633 f.; Carlé (2007), p. 2226.

### iii. Die Überwachungsgesamtrechnung

It has already been explained in the previous chapter that the Data retention Directive was not only a case for the CJEU. While the measures of the Directive were challenged twice before the CJEU, the laws implementing the Directive into national laws were also challenged individually in the Member States. Several national constitutional courts invalidated the local data retention laws for violation of the right of citizens to protection of privacy, before the CJEU invalidated the Data retention Directive, on which those laws were originally based. One of those cases was heard by the BVerfG in Germany.

As has been shown already in the previous chapter,[2006] the German Constitutional Court invalidated the provisions implementing the Data retention Directive for much the same reasons as for which the CJEU later invalidated the Directive itself. But in addition, the Constitutional Court went a step further. It emphasized that the storage of data about customers or users without sufficient cause for suspicion could not be the norm, and that it should, instead, constitute only a narrow exception to the rule, applicable only where absolutely necessary.[2007] The Court clarified that a prohibition of the total surveillance of the population's private lives is not simply demanded by the right to privacy guaranteed in article 2 GG, but part of the constitutional identity of the German federal republic.[2008]

Furthermore, the Court stated that a measure of precautionary surveillance cannot be examined in isolation, but must always be seen in the context of the totality of the existing collections of data on the citizens.

> "The introduction of a duty to store telecommunications traffic data may therefore not serve as a blueprint for the creation of further data pools as a precautionary measure. Instead, the legislator is obliged to exercise a greater restraint in considering new duties or authorities to store personal data with regard to the totality of the various existing data pools. […] Precautionary storage of telecommunications traffic data also



2006 See section (b) of Chapter IX above.
2007 BVerfG, 1 BvR 256/08 [2010], paragraph 218.
2008 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Schwartz (1968), p. 751; Hohmann-Dennhardt (2006), p. 548.

> considerably reduces the latitude for further data pools created without cause, including collections introduced by way of European Union law."[2009]

The German Constitutional Court thus favours a very different, holistic approach from the one applied by the CJEU. According to the Constitutional Court, the lawmaker is forced to take account of all existing surveillance measures before considering the introduction of an additional measure.[2010] Such an examination of the landscape of surveillance is directly opposed to the fragmented approach currently applied.

**iv. Privacy and Dignity**

Evaluating such a landscape of surveillance would be a difficult task, however. There are so many laws in existence that introduce surveillance measures,that it is difficult to determine the whole extent of measures that intrude upon the right to privacy of the population. For Germany alone, the NGO *digitalcourage* has identified 41 laws passed since 2010 which create additional surveillance, or otherwise intrude upon the privacy of the population or parts of the population.[2011] Those laws include laws concerning the data of third country nationals and asylum seekers, laws facilitating the information exchange among law enforcement agencies within the European Union, laws governing medical assistance, transport and traffic, and, of course, financial data.[2012] It can be expected that the situation in most other Member States is comparable, with an equal amount of surveillance measures applied to all or parts of the population.

All of those individual measures could be considered to be based on a law and genuinely address a legitimate objective in the general interest.[2013] The essence of the rights to privacy and data protection will likely not be held to be affected by any of these laws, when one of them would be evaluated. The Court may even find the infringements by these measures to be proportionate to the aim. Therefore, each of those laws could be legitimately applied.

2009 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Skouris (2016), p. 1364; Möllers/Redcay (2013), p. 420; Linke (2016), p. 891.
2010 See also Baum (2011), p. 596; Roßnagel (2010), p. 547.
2011 See https://digitalcourage.de/blog/2016/materialsammlung-ueberwachungsgesamtrechnung#staat, last accessed 3 January, 2018.
2012 It should be noted that surveillance carried out by private undertakings based on their business models was not considered in this list.
2013 Schröder (2016), p. 642.

Therefore, the amount of surveillance and intrusions into the privacy of the population is allowed to grow continually and practically unrestrictedly. In particular, the importance of data processing to the daily life of an average person has greatly facilitated the secret and undetected intrusion into the rights to privacy and data protection.[2014] The fact that access to digital services is absolutely necessary for many people, particularly for communication and information purposes in both professional and private life, creates an imbalance because this necessity on the part of the consumer is easily and readily exploited for surveillance by private and public entities.

A particular role in the exponentially growing mass surveillance is played by the collections of data by private entities.[2015] Many businesses are in the process of building immense databases of customer data. For instance, banks are collecting tremendous amounts of information on a customer's financial situation,[2016] medical service providers and insurances are collecting data on a person's health, internet services providers are collecting data on the information accessed by their customers, and the amounts of data collected by providers of social media service providers is so vast that the significance of those data collections can hardly be estimated at this point. However, aside from the data protection and privacy risks of these data collections in the hands of private entities alone, an aspiration of the authorities to tap into these data sources can also be detected.[2017] Depending on the instrument, access is to be gained either directly, as in the case of the Data retention Directive, or, as in the case of the Anti-money laundering Directive, by "instrumentalisation and integration of the financial sector into the investigations and prosecution objectives of the authorities."[2018]

The right to privacy is different from most other fundamental rights recognized in the Charter, as intrusions may be accomplished on a grand scale, covertly, without the knowledge of the data subject. Intrusions into other rights may be more quickly felt by those affected, and protested against. For instance, an intrusion into



2014 Hamacher (2006), p. 633.
2015 Boehm (2012), p. 341 f. See also Einzinger/Skopik/Fiedler (2015), p. 728.
2016 The data collected by banks in accord with their obligations under the Anti-money laundering Directive were discussed in Chapter II section (e), and evaluated in Chapter IX.
2017 Hamacher (2006), p. 633; Cannataci (2013), p. 6 f. In this context, it should be pointed out that *Simitis* has warned of the desire of the government to use databases compiled by commercial actors early on. His concerns were brushed aside at the time. See Bull (2006), p. 1620.
2018 Hamacher (2006), p. 633. See also Boehm (2012), p. 342.

the right to property probably weighs more heavily in the opinions of many people than an intrusion into the right to privacy, simply because the consequences of an intrusion into the right to property are usually noticed immediately by the individual. Intrusions into the right to privacy are often more slowly and more subtly felt by the data subject.

It is clear that the aggregate mass of all of the existing infringements and intrusions combined is unprecedented.[2019] The situation is exacerbated by the fact that these infringing measures are based on laws granting powers of surveillance, and on the business models of private entities. Both legal and illegal intrusions into the right to privacy occur copiously. Intrusions may be caused by positive law authorizing the intrusion, or it may be caused by the absence of proper protection of the privacy and data of individuals.[2020] Data processing operations may be conducted openly or covertly. The situation has grown into a completely intransparent and opaque web of surveillance measures, which no data subject can escape. In combination, this amount of surveillance cumulatively is well capable of adversely affecting the essence of the rights to privacy and data protection.

The danger of this situation lies in the first place in the much-cited close connection of the right to privacy with the right to human dignity: "Human dignity is inviolable",[2021] and therefore allows for no intrusions. A situation in which a right so closely connected to that right as the right to privacy is constantly further intruded upon is therefore at the same time an infringement of the right to human dignity.[2022] This is starkly at odds with the inviolability of human dignity under Article 1 of the Charter.

Secondly, the rights to privacy and data protection are of extraordinary importance for many other rights. This concerns in particular the freedom of expression and the general freedom of the individual. This is the reason why it is considered that a free and democratic society can only absorb a certain level of surveillance before it loses its character as both free and democratic. The reason for this danger are the

2019 See also Bull (2006), p. 1617.
2020 See Chapter V above.
2021 Article 1, first sentence of the Charter of Fundamental Rights. See also Lynskey (2014), p. 572.
2022 Hirsch (2008b), p. 89.

chilling effects that are caused by excessive intrusions into the right to privacy.[2023] An individual who expects his behaviour to be subject to surveillance may often prefer not to stand out and avoid to show certain behaviour which may cause him to be singled out by the authorities.[2024] The absence of a meaningful protection of the right to privacy therefore has the potential to hinder individuals in exercising other human rights, particularly the freedom to develop one's personality,[2025] and the freedoms of speech and expression.[2026]

To repeat the words of the ECtHR at this point: "In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse."[2027]

This condition of safeguards is often not met. As has been shown above, a major criticism of the Anti-money laundering Directive is its lack of meaningful safeguards for personal data, particularly for special categories of data.[2028] The volume of different measures based on different laws exacerbates this situation. The individual is unable to protect his or her privacy against all of the different measures he or she is confronted with. The safeguards that do exist fail to offer meaningful protection. The demand of the ECtHR that there must be adequate and effective safeguards is therefore not met. This demand of the ECtHR is, however, also not necessarily applicable to the cumulative effect of intrusions into the right to privacy, due to the Court adjudicating on only one legal instrument at a time.

**v. A Holistic Approach**

The absence of meaningful safeguards against this cumulative effect of intrusions into the right to privacy should be regarded as a grave threat to the fundamental rights of the individual. The failure of traditional tools to protect the individual's privacy from this threat makes it necessary to consider whether there are other mechanisms which may be employed to improve the protection of individual.



2023 See CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 101. See also Tinnefeld (2007), p. 628 f.; Maras (2012), p. 72 f.; Hirsch (2008b), p. 89.
2024 Martini (2009), p. 841; Benn (1984), p. 227 f.; Maras (2012), p. 74.
2025 Tinnefeld (2011), p. 589 f.
2026 CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 101.
2027 ECtHR Case of *Roman Zakharov v. Russia* [2015], paragraph 232. See also Article 29 Working Party, Working Document 1/2016, p. 5; Bülow (2013), p. 609; Korff (2014), p. 108; Galetta (2013), p. 10.
2028 See the fifth and thirteenth concern discussed in Chapter IX above.

The German Constitutional Court therefore suggests a holistic approach in which the combined effect of all surveillance measures must be surveyed. The approach favoured by the BVerfG could also be characterised as an addition to the proportionality standard:[2029] In the first place, all individual measures that intrude upon the rights to privacy and data protection must fulfil the applicable standards. They must be based on a law which aims at achieving an objective in the public interest and the measures must not go beyond what is necessary in order to achieve the objective. In a further step, however, the proportionality of the entire applicable existing surveillance framework could be examined, in order to determine whether an additional measure can be accounted for. Only when the lawmaker, after an assessment of the existing surveillance landscape, comes to the decision that a further measure can be absorbed by society, may this measure in fact be introduced.[2030] Such a holistic approach would make a piecemeal legal surveillance structure as outlined above impossible, and add considerable protection for the privacy of the population, since the lawmaker would be forced to review the overall level of surveillance periodically. Such a review would also achieve a greater transparency for the population, and would imply that surveillance measures can also be rolled back, rather than only ever being increased with each newly introduced law.

The holistic approach would protect the privacy of individuals, and especially the essence of this right. The inviolability of the aspects of privacy which are related to human dignity makes the meaningful protection of these aspects a task of very high importance. The BVerfG has made it clear on several occasions that it takes inviolability of human dignity[2031] and the strict protection of the intimate sphere of an individual's privacy very seriously.[2032] The proper protection of human dignity and the aspects of an individual's privacy falling into the intimate sphere therefore need to be protected comprehensively and meaningfully, including from the cumulative effect of a large number of infringements.

If and how such a holistic approach is going to be applied remains to be seen. The German lawmaker has in any case not yet begun with the implementation

2029 Article 29 Working Party, Opinion 1/2014, p. 21 f. The Article 29 Working party also appears to see the holistic approach connected more closely to proportionality than to the essence of a right. See also Roßnagel (2010), p. 547.
2030 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Gietl (2010), p. 403; Roßnagel (2010), p. 547.
2031 See for instance BVerfG, 1 BvR 2378/98 [2004], paragraph 121.
2032 See for instance BVerfG, 1 BvR 1689/88 [1994], paragraph 20 ff.

of such a holistic approach. However, slowly, the calls for such an approach are increasing,[2033] also on a European level. The Article 29 Working Party, for instance, included a recommendation of a holistic approach in an Opinion of 2014:

> "Particularly after 9/11 the European legislator(s) have been extremely active adopting new measures limiting the rights to privacy and data protection in the [Area of Freedom, Security and Justice]. This development makes it particularly important to take a holistic viewpoint when assessing the interference with privacy and data protection of a new legislative proposal. In order to say whether a new legislative proposal is still proportionate, it is necessary to assess how the new measure would add to the existing ones and whether all of them taken together would still proportionately limit the fundamental rights of data protection and privacy."[2034]

This increasing interest bodes well for a potential re-evaluation of the protection which the rights to privacy and data protection are receiving under the current framework: A discussion on the proper protection of these rights alone is already valuable in itself. Only a thorough discussion can yield the insight needed to design a framework under which human rights are comprehensively protected, in accord with legitimate limitations of those rights in the public interest.

**vi. Applying a Holistic Approach**

It almost goes without saying that a holistic approach to surveillance and the right to privacy may not be the easiest approach to apply in practice. The assessment of the landscape of surveillance would have to be undertaken. A trusted entity would have to be tasked with mapping the landscape of surveillance and keeping this map up to date.

It would not be necessary, however, to create a new authority for this task. The data protection authorities both on the European level as well as on Member State level have proven themselves very capable of carrying out all of the tasks they

2033 See the remarks by *Gillian Triggs*, quoted in Wahlquist (2017).

2034 Article 29 Working Party, Opinion 1/2014, p. 21 f. However, the Article 29 Working Party here only brings in this holistic approach at the very end of its Opinion on the application of necessity and proportionality and data protection within the law enforcement sector, neglecting a deeper look into this approach at this point, and omitting all references. It can therefore not be determined how this conclusion was reached.

are already charged with, often under imperfect circumstances. These authorities would be ideally suited to carry out this mapping of the landscape of surveillance, of keeping the map up to date, and of making a preliminary assessment as to the gravity of interferences.

A futher question which remains to be settled is which interferences would need to be included in this map. One may argue that the landscape of surveillance should only include interferences which are based on a positive law. In this way, the landscape of surveillance would be directly linked to the accountability of the state for the surveillance measures it introduces. However, a limitation of the map to interferences of the state based on a law would necessarily leave many other measures of mass surveillance in fact applied out of the picture. The surveillance of the behaviour of individuals online by private entities for instance, is a concern which should be accounted for. In the first place, private entities process vast amounts of data and are in the process of driving the development of Open Data and Big Data Databases.[2035] In the second place, much of the data processing carried out by private entities is not so much based on a law but largely based on the absence of meaningful data protection safeguards for data subjects.[2036] However, this inactivity is also a factor for which the state must be held accountable. Finally, the tendency of the state to tap into databases created by private entities has been outlined earlier in this chapter. As *Boehm and De Hert* observe, "almost all existing databases have multiple functionalities."[2037] The application of surveillance measures and the establishment of large scale databases are always attractive to be utilised for the purposes of law enforcement agencies and the secret services of Member States. Therefore, it should be considered to include all surveillance measures applied by private entities into the map as well.

Finally, it should be emphasised that the level of surveillance faced by individuals in society may reach a critical point, in which no additional measures of mass surveillance may be added. When this point would be considered to be reached, the lawmaker would therefore be limited in its competence to add legal provisions authorising new surveillance measures until it has limited the existing surveillance in such a way that the level of surveillance applying to society is lessened. This

2035 See Chapter VII above. See also on Big Data and privacy Leonard (2014), p. 53 ff.
2036 See the remarks made on insufficient data protection safeguards in Chapters II, V, VII, and IX.
2037 Boehm/De Hert (2012), p. 2.

may be achieved by either removing or limiting some of the existing surveillance measures in order to lessen the density of surveillance. It may also be achieved by strengthening the rights of the data subjects and safeguards connected to the processing of data.[2038]

The interpretation of the landscape of surveillance and the burden of this surveillance on society should be left up primarily to the lawmaker. The democratically legitimised lawmaker is principally in the best position to appreciate its own measures, particularly where they reflect political choices. However, the Courts should be in the position to review the choice made by the lawmaker. This is the same situation as in the application of the principle of proportionality: It is principally left to the lawmaker to design legal measures in such a way as to be compatible with the principle of proportionality. However, the lawmaker may sometimes err in its assessment. Therefore, the proportionality of any legal measure may be reviewed by the Court. In the same way, the assessment of the landscape of surveillance made by the legislator should be subject to the reivew by the competent Courts.

Again, such review would be closely connected to the principle of proportionality: the Court would need to formulate certain criteria by which the burden caused by the cumulative effect of the existing surveillance measures is reviewed. This test may consider the effectiveness of the surveillance measures, their intrusiveness, the remaining spaces in which individuals may move without being affected by such measures, and the impact of the cumulative effect of all surveillance measures combined on the essence of the right to privacy of individuals.

It can be said, therefore, that the application of a holistic approach would demand some administrative measures to accommodate it in the existing framework. But taking into account the potential gains in terms of an increased level of protection of the rights to privacy and data protection, the necessary changes can be considered a low hurdle to its implementation.



**vii. Constitutional Identity**

In this context, it should be pointed out that it is not entirely new that the German Constitutional Court shows itself dissatisfied with the work of the European

2038 See the discussion of a right not to be identified in Chapter VII above.

lawmaker, and the German envoys to the European lawmaker.[2039] The BVerfG has a long history of criticizing an insufficient human rights standard prevalent in implementations of European legislation into national law. Naturally, this criticism is in the first place directed at the German legislator itself, which should have been more careful in drafting the implementation, and at the German government, which is involved in the decision making process on the European level.

The first major conflict is expressed in the *Solange* decision of the BVerfG of 1974,[2040] in which the BVerfG officially stated that it would disregard the doctrine of supremacy of European law developed by the CJEU ten years earlier[2041] insofar as European law collided with the human and civil rights proscribed by the German Constitution.[2042] The Court specified that as long as on the European level there existed no democratically legitimized catalogue of human rights of equal extent as that of the German constitution, it would continue to measure all laws, including those of European origin, which were applicable to the German population, by the standards of the German Constitution, with the possible result that the law may be declared unconstitutional and therefore invalid.[2043]

After this deficiency had been remedied on the European level and acknowledged by the BVerfG in 1986,[2044] the rift became less visible, but did not quite cease to exist. The BVerfG is still of the opinion that a European law, which is in conflict with the guarantees of the Constitution, is not covered by the European doctrine of supremacy, and could be declared invalid by the BVerfG if so necessary. This view is shared also by several other constitutional- or supreme courts in other Member States.[2045] Therefore, although the BVerfG has been avoiding open confrontation with the CJEU, the Court's decisions often emphasise the obligation of the German authorities to the German constitution, and specifies the way in which the authorities should comply with these obligations.[2046]

2039 Hornung/Schnabel (2009b), p. 119; Lewinski (2012), p. 567 f.; Kahler (2008), p. 452.
2040 BVerfG, 2 BvL 52/71 [1974]. See also Fisahn/Ciftci (2016), p. 365 f.; Leutheusser-Schnarrenberger (2016), p. 355; Lewinski (2012), p. 569; Roßnagel (2010), p. 546.
2041 CJEU Case 6/64, *Flaminio Costa v E.N.E.L.* [1964].
2042 See also Ronellenfitsch (2009), p. 460 f.; Dix/Petri (2009), p. 534 f.
2043 BVerfG, 2 BvL 52/71 [1974], paragraph 285. See also Fisahn/Ciftci (2016), p. 369; Jacobs (1999), p. 1 f.; Ronellenfitsch (2009), p. 460 f.; Roßnagel (2010), p. 546.
2044 BVerfG, 2 BvR 197/83 [1986].
2045 For example Poland and Denmark. See Möllers/Redcay (2013) p. 419 f. with further sources.
2046 Möllers/Redcay (2013) p. 420 f.

Such clarifications are also contained in the BVerfG's data retention decision. The Court here clarified that the prohibition of a total registration of the exercise of the population's rights is part of the constitutional identity of the German federal republic.[2047] The Court does not stop there, however, but continues with the demand of the authorities to ensure the protection of this constitutional identity not only nationally, but also on the European and international level.[2048] Finally, the Court explicitly warns the German authorities that by introducing data retention in the field of telecommunications data, its options for the introduction of further surveillance measures is significantly limited, and that measures introduced by European law are by no means exempted from this limit.[2049] The Court therefore already explicitly anticipated and negated the obvious excuse that the German lawmaker is obligated to implement a certain directive as demanded by the European Union.[2050]

This point is of some importance. The judgment can thus be understood to place a positive obligation on Germany to work towards greater restraint in the introduction of surveillance measures not only within the European Union, within whose law-making process Germany has considerable influence, as well as in the international arena, which would also include the FATF, of which Germany is also a Member. It should be pointed out that the fourth Anti-money laundering Directive was adopted after this judgment. It is not apparent that such a survey of the landscape of all existing surveillance measures has taken place before the adoption of the new directive, nor that the German representation on the European level has considered itself limited by a consideration of the warning directed to it by the judgment. Future case law of the BVerfG is expected with great interest.

## e. Conclusion



The right to privacy is one of the rights which need to be afforded a particularly high level of protection, because they "are of a structural importance for the functioning

2047 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Hohmann-Dennhardt (2006), p. 548; Roßnagel (2010), p. 546.
2048 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Streinz (2011), p. 602.
2049 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also Hornung/Schnabel (2009b), p. 119.
2050 See also Leutheusser-Schnarrenberger (2014), p. 590.

of the democratic system and discourse".[2051] A framework for better protection of the rights to privacy and data protection would serve to add a significant layer of protection not only of those rights, but of the right to human dignity, and of other fundamental freedoms indispensable for a free and democratic society, such as the freedom of the press, the freedom of expression,[2052] and the freedom of speech.

This position of the right to privacy should be kept in mind at all times. It emphasises the need for a high level of protection of this right. Particularly the essence of the right to privacy must under no circumstances be encroached upon. This is clearly demanded in the text of the Charter. The term essence in itself, however, hints at the most important core values of the right in question, at the very heart of the right to privacy. The protection of the essence of the right to privacy can therefore be seen, in the context of infringements into the right to privacy, as a final strong safeguard against infringements which were not caught and filtered out by means of the other traditional safeguards.

However, the essence of the right to privacy is at risk due to the cumulative effect of the numerous existing different infringements into the right to privacy. The data subject lacks meaningful safeguards against the combined effect of all of these measures. The traditional defence of the principle of proportionality is ineffective as a measure of protection. Whenever one individual law is challenged based on disproportionate interference, the framework currently in place will only allow for that particular legal measure to be considered by the Court. Therefore, the test currently in place allows for the introduction of a far-reaching, finely meshed web of individual surveillance measures, which, in combination, create a situation which the Court would not have accepted if it had been created by one piece of legislation. The aggregated mass of such individual surveillance measures are well capable of adversely affecting the essence of the right to privacy. If the CJEU were to introduce a holistic approach as envisioned by the BVerfG, it would gain an effective tool that could be used to protect the population from slowly further encroaching infringements into their privacy.

Due to the ever increasing amount of surveillance with which the individual is confronted, the holistic approach should be considered to be a valuable defence

2051 Wehlau/Lutzhöft (2012), p. 49.
2052 See also Maras (2012), p. 76; Schmale/Tinnefeld (2017), p. 347.

of the privacy, identity, and ultimately the personal freedom of the individual. Indeed, it may be the *only* viable approach with which the individual's privacy can truly be protected.

# Chapter XI

## Conclusion

## Outline:

a. Answers to the Research Questions
    i. Preliminary Questions
    ii. Theoretical Framework
    iii. The Main Research Question
    iv. Impact
    v. A Holistic Approach
b. Conclusions and Recommendations
        (1) The Sweeping Scope of the Anti-money Laundering Measures is Incompatible with Privacy and Data Protection.
        (2) There is Insufficient Regard for Privacy and Identity Issues in Financial Transactions.
        (3) Alternative Transactions Systems do not Provide Increased Privacy to Users.
        (4) The Proportionality Assessment is Currently the Most Relevant Test, but it has Significant Weaknesses.
        (5) The Proper Protection of the Essence of Privacy Requires a New Test.
c. Developments in the Field
    i. Recent Developments
    ii. Future Developments
    iii. Concluding Remarks: Further Research

## a. Answers to the Research Questions

### i. Preliminary Questions

Over the course of this thesis, a number of research questions and groups of sub-questions were addressed and researched in detail in order to create the framework within which to discuss the research problem. In the first place, this research discussed the anti-money laundering framework in detail, including its origin, application, and a preliminary critique.[2053]

Chapter II showed the origins of the anti-money laundering legislation in the 1970s in the United States and in Europe, slowly evolving into an international network of remarkable size, with numerous international instruments determining the approach to money laundering and terrorist financing which is now followed at least to some extent in almost all countries across the world.[2054] This approach is also followed in the European Anti-money laundering Directive. According to this approach, financial services providers of all descriptions are involved in the detection of potential money laundering operations. The obligations falling onto those services providers are fourfold: in the first place, all customers must be identified. Secondly, all transactions must be monitored in order to be able to filter out any suspicious transactions. If any suspicious activity is detected, the obliged entity must in the third place forward this information to the Financial Intelligence Unit and comply with requests for information if the FIU requests any data. In the fourth place, information identifying the customer and transaction records must be retained for five years after the end of the business relationship. This rigorous anti-money laundering regime is, however, viewed critically by many commentators.[2055] The main points of critique concern the costs involved, the lack of effectiveness, and the serious interferences with the privacy and data protection rights of the customers.

The two primary preliminary questions concerning alternative transactions systems were firstly, what they are and how they function,[2056] and secondly, if and

2053 The first set of research questions was answered in Chapter II.
2054 North Korea and Iran are the only two countries which are fully blacklisted for non-compliance with the FATF standards. See http://www.fatf-gafi.org/countries/#high-risk (last accessed 3 January, 2018). See also Hülsse (2008), p. 461 f.
2055 See Chapter II above.
2056 This research question was answered in Chapter III.

how they are covered by the anti-money laundering framework.[2057] The detailed explanation of the two transaction systems given in Chapter III has shown that virtual currency systems, the first transaction systems that were addressed by this thesis, are a novel system for transactions, based on a peer-to-peer system and cryptography. Bitcoin served as a primary example. Its open structure eliminates the need for a central authority such as a bank in order to reliably transfer funds. The second group of alternative transaction systems that was addressed in this thesis, was that of informal value transfer services, particularly Hawala. Hawala is a network of service providers transferring funds in such a way that the funds do not move physically. Hawala is fast, cost-effective, secure, and culturally convenient to its users, who are for the most part members of the expatriate community from countries in which Hawala is the dominant financial service.

Both systems can therefore be employed in order to transfer value in the same way as the banking sector is used, but their services are preferred by the users of each system for different reasons. There may be persons who avoid the conventional banking sector for ideological reasons, rejecting this aspect of the capitalist society, the surveillance that customers are subjected to, or the internal mechanisms of a bank which might be conflicting with one's religious views. Virtual currencies are at this point in time also particularly interesting as a vehicle for investments, or to conclude purchases of illegal goods and services on the dark web. Furthermore, the group of undocumented immigrants in Europe is often overlooked and not much considered in statistics or policy-making. However, this group of people certainly does exist, and members of this group certainly do need to have access to basic banking services. But, the fact that they cannot prove their identities with official documents excludes them from the conventional banking sector, often leaving Hawala as the only viable option.[2058] In addition, the services of alternative financial services providers may be faster, cheaper, and more reliable than those of the conventional banking sector, depending on what sort of transaction is carried out, and particularly on where the counterparty to the transaction is located.

2057 This research question was answered in Chapter IV.

2058 Whether virtual currencies may also become a viable option in such circumstances is an interesting question. Virtual currencies may provide the same services as Hawala, as in principle only a smartphone with internet connection is needed for access. There is as yet no reliable research on the adoption of virtual currencies by migrants, but it is a potential development which will be watched with interest.

In Chapter IV, the application of the anti-money laundering measures to alternative transaction systems has been shown. Although the scale of surveillance is immense, the Anti-money laundering Directive is unable to cover alternative systems for financial transactions in a similarly comprehensive way as it does the conventional banking sector.

In the first place, virtual currencies cannot be covered comprehensively by the terms of the Directive. Virtual currencies elude the anti-money laundering approach by lacking a central authority which could be obliged to apply the anti-money laundering measures. Virtual currencies are in fact not an institution but in essence simply a computer programme run by a network of individuals around the world. Therefore, the system itself is not covered. The only aspect of virtual currencies currently already covered by the Directive are service providers, such as exchange services. Those service providers can already be classified as obliged entities under the terms of the fourth Anti-money laundering Directive, and the proposed fifth Anti-money laundering Directive would add the positive aspect of introducing legal certainty for these service providers by explicitly covering them as obliged entities. Users can, however, use virtual currencies without making use of these services, or they may turn to service providers located in a state with weak anti-money laundering oversight mechanisms. This limits the potential benefit of the coverage of those systems by European law for the purposes of anti-money laundering.[2059] The coverage of decentral virtual currency systems like Bitcoin by anti-money laundering legislation is therefore incomplete.

Hawala is at once different and similar in this case. The Hawala system is in essence a large network of interconnected persons, very similar to virtual currencies, except that hawaladars can potentially offer their services without a sophisticated technological infrastructure. Hawaladars in Europe cater first and foremost to the members of the expatriate communities they themselves belong to, offering their services to people wishing to send remittances to their home country. The very simple nature of the service they provide allows them a large degree of flexibility and independence, and makes them resilient to attempts at regulation.[2060] The fact that funds need not move physically, combined with the fact that hawaladars



2059 See the discussion of virtual currencies in Chapters III and IV above.
2060 See for details the discussion of informal value transfer systems in Chapters III and IV above.

generally operate underground and in noncompliance with the applicable financial regulation, also causes the incomplete coverage of this system. The activities of a hawaladar are difficult to detect by the authorities and even more difficult to sustainably prevent, considering the great demand for the services of hawaladars. Therefore, it can be stated that the anti-money laundering approach only really matches the parts of the financial sector for which it was designed, leaving large gaps in oversight over alternative services.

**ii. Theoretical Framework**

Following the answer to this first set of sub-questions, the second set of sub-questions was addressed. This set concerned the theoretical framework within which the main research question was answered. The first question concerned the rights to privacy and data protection: What is the content of these rights?[2061] This concerns especially the proper protection of these rights, as the assessment of their protection was to be an integral part of the main research question.

Chapter V was dedicated to answering these questions. The rights to privacy and data protection are supporting pillars of a free and democratic society, enshrined in article 8 ECHR and articles 7 and 8 of the Charter of Fundamental Rights of the European Union. These rights protect the individual from intrusions into his or her private life and from illegitimate processing of his or her personal data. In order to ensure the protection of these rights, the data subject is endowed with a number of rights under the GDPR and, to a somewhat lesser extent, the Police and Criminal Justice Authorities Directive. These instruments add details to the protection of the rights to privacy and data protection by codifying a number of rights of the data subjects, fundamental principles for the protection of data, and other rules concerning data processing.

In essence, all data relating to an identified or identifiable person is protected under the data protection rules. Anonymous data, on the other hand, is in principle excluded from the scope of protection of the right to data protection. This definition, however, raises the question what the concept of identity really means. Sub-questions relevant in this context were, what is the content of the two concepts of identity and

2061 This research question was answered in Chapter V.

anonymity, and how do those concepts relate to privacy and data protection? How is the identity of a person involved in financial transactions?[2062]

These questions were answered in Chapters VI and VII. In those chapters, it was shown that the concept of identity is complex, and that it is defined very differently in different scientific disciplines. The sociological model used in this thesis was to consider an individual's personal identity and his or her social identity. A personal identity is formed by the personal attributes an individual places particular emphasis on, while a social identity is formed along the lines of how the rest of society perceives an individual. In legal terms, the focus of identity in the first place lies on the question how one individual can be distinguished from all other individuals. While the state may achieve this task by assigning each resident a personal identification number, it may also be achieved by the combination of name and date and place of birth or other identifiers. At the same time, other identifiers may serve the same purpose of singling an individual out from the rest of the group, particularly by third parties. Where an individual is identified or identifiable, the data protection legislation is applicable, with all the rights, restrictions, and principles contained therein. Where an individual is anonymous, on the other hand, the data protection legislation is in principle not applicable. Data is anonymous when the data cannot be linked to an identified or identifiable person. However, in many instances even anonymised data can, where the anonymization process was not thorough enough, be linked to an identifiable person. There is so much data available on identified and identifiable persons already, that the possibility of linking previously anonymous data to an identified or identifiable individual can hardly be excluded.

The identity of an individual is also always involved in financial transactions. The Anti-money laundering Directive explicitly forbids anonymous accounts, and demands that all obliged entities fully identify all of their customers. The anti-money laundering framework speaks of identifying customers in a legal sense, that is, customers must prove their identity by means of an official document uniquely identifying them. However, the aspects of personal and social identity are also closely connected to the measures contained in the Directive. When a customer begins a long-term business relationship with a service provider, such as is the



2062 These research questions were answered in Chapter VI (identity) and Chapter VII (anonymity).

case when a customer opens a bank account with a credit institution, the service provider will quickly accumulate a large amount of personal information about this customer. The personal information is here not only limited to identifying information as contained in one's official identity document, but also information pertaining to other aspects of a person's identity. In this way, the transaction history of a bank customer will often allow for accurate inferences to be drawn concerning the customer's personal circumstances, including, under certain conditions, his sexual preference, religious conviction, political opinion, and many other aspects. The transactions of the customer are at the same time subject to anti-money laundering measures, which equally affects all transactions containing sensitive personal information.[2063]

The impact of an individual's identity on the choice of a financial transaction system should also not be underestimated. The difficulty some members of the population face when a proof of their identity is demanded has already been mentioned. In addition to that point, a person's social and personal identity can play a major role in their choice for a transaction system. As has already been mentioned earlier, there may be persons who avoid the conventional banking sector and instead decide to opt for a different transaction system. Religious and ideological views and concerns can play a big role in the customer's choice for virtual currencies or informal value transfer services. The concept of identity is, however, of interest also in other respects. In the first place, one of the main obligations faced by obliged entities is to identify their customers. How a customer proves his or her identity is one aspect of this concept. Another aspect of the concept is, however, its intimate connection with the notion of privacy.[2064] For instance, one's identity is to a large extent shaped by traits which are directly linked to categories of data which are considered sensitive. An individual's sexual orientation, medical condition, and religious orientation are often large factors in their identity, but information about these factors is considered sensitive. Information relating to these intimate and sensitive aspects of an individual's identity can also be found in the customer's transaction history.[2065]

2063 See Article 29 Working Party, Opinion 14/2011, p. 26 on sensitive information.
2064 See also Chapter VI for the connection between privacy and identity.
2065 For instance when the customer makes donations electronically to religious foundations, when medical bills are paid, or when membership fees for labour organisations are deducted.

This direct connection between the anti-money laundering framework and the customer's identity, privacy and personal data, should not be lost out of sight. The connection between the legitimate interest in protecting the customer's identity and privacy and the erosion of this protection by the anti-money laundering measures is strong, as the identity of the customer influences not only his or her choices, but is also reflected in his or her behaviour, including in financial transactions. At the same time, there are hardly any options for the customer to protect his or her identity. Therefore, one of the main conclusions reached in this thesis is that there is insufficient regard for privacy and identity issues in financial transactions.[2066]

Finally, prefacing the answer to the main research question, the principle of proportionality was examined in detail. What precisely is the content of the principle of proportionality as applied by the CJEU and ECtHR, and how has it evolved over the course of recent case law?[2067] Chapter VIII was devoted to these questions. In essence, the principle of proportionality demands that any measure should not interfere with the rights of the population more than is necessary in order to achieve the aim pursued by that measure. The CJEU and ECtHR apply the principle slightly differently. The CJEU applies a test of three steps. It asks first, whether a measure is suitable to achieve the aim it pursues, secondly, whether the measure does not go beyond what is necessary to achieve the aim, and thirdly, whether the conflicting interests involved are properly balanced. The ECtHR, in contrast, has not yet chosen to develop a standard test. The case law of the ECtHR generally concentrates on the applicable safeguards accompanying a measure, and the 'relevant and sufficient reasons' given by the lawmaker in order to show that a measure is necessary in a democratic society and addressing 'a pressing social need'. When applied to a given measure, however, the different tests of the CJEU and the ECtHR generally yield the same outcome.

### iii. The Main Research Question

The main research question was whether the anti-money laundering measures as currently applied across Europe properly respect the rights to privacy and data protection.[2068] This question was addressed and answered in Chapter IX. According



2066 See also conclusion (2) discussed below.
2067 This research question was answered in Chapter VIII.
2068 This research question was answered in Chapter IX.

to article 52 of the Charter of Fundamental Rights of the European Union, a measure is in accord with human rights only if it is provided for by law, respects the essence of the right, and if the intensity of the interference of the measure with human rights is proportionate to the aim it pursues. The proportionality assessment often lays at the core of the assessment. Questions to be addressed to answer the main research question were, in what ways do these measures interfere with the rights to privacy and data protection? Do the measures pursue a legitimate aim, and are they justified? What are the concerns that the anti-money laundering measures raise, particularly in terms of privacy and identity, and particularly in the light of the latest case law of the CJEU?

The measures of the Anti-money laundering Directive interfere with the privacy of individuals in several different ways. Individuals are identified when the obligations of the Anti-money laundering Directive are triggered, and copies of the documents are retained by the service provider for five years after the end of the business relationship between the customer and the service provider. Furthermore, all transaction are monitored by the service provider, and a transaction history is retained after the end of the business relationship. The processing of data for this purpose and the retention of the transaction record constitute further interferences. When a transaction appears suspicious, the Financial Intelligence Unit is informed of it. The transmission of data to the FIU is another interference. The inclusion of customer information in central databases should also be seen as an interference. Considering that almost every inhabitant of the European Union depends on financial services to some extent, and that the rules of the Directive therefore comprehensively affect the entire population, this thesis argued that the interference of the Directive should be considered particularly serious.

It may be argued that the anti-money laundering measures pursue the legitimate aim of preventing and facilitating the detection and investigation into serious crime and are therefore justified. The interest in curbing crime is certainly legitimate. However, the interest of the population in protecting their privacy and personal data is equally justified. Therefore, it is particularly important that the measures do not go beyond what is necessary, and that a balance is struck between the conflicting interests.

The design of the measures raises some concerns about their compatibility with the rights to privacy and data protection. A list of seventeen concerns has been compiled, the most striking of which are the mass surveillance character of the measures, the lack of safeguards for sensitive categories of data, the excessive retention periods, and the lack of procedural safeguards ensuring the protection of the rule of law.[2069] These concerns were analysed by comparing the existing case law on privacy, particularly the CJEU's judgments on the data protection Directive, with the measures of the Anti-money laundering Directive. Based on the Court's existing case law, it is argued in this thesis that the measures of the Directive go beyond what is necessary to achieve the aim pursued. The measures cut too deeply into the privacy of customers. In addition, the rights to privacy and data protection are not properly balanced with the interest in facilitating the fight against serious crime. Therefore, the measures of the Anti-money laundering Directive do not properly respect the principle of proportionality.

The fifth Anti-money laundering Directive is only going to aggravate the situation upon entry into force. It is going to establish registers in which individuals will be included, add specific rules covering virtual currencies, and close remaining loopholes. The finding that the Directive is disproportionate is significant because the Anti-money laundering Directive covers the entire European population. The number of people with access to a bank account is growing steadily toward one hundred per cent, bringing with it a comprehensive surveillance of the financial activity of the population. In addition, the anti-money laundering measures are not only applied by the banking sector itself, but also by other professions, such as lawyers, tax accountants, insurance providers, and auditors. The mesh of surveillance introduced by the Anti-money laundering Directive is therefore very fine and comprehensive. According to the assessment conducted in this thesis, it is considered very likely that the CJEU would invalidate the Directive when it is challenged.

**iv. Impact**

The impact of this negative proportionality assessment was also considered in a set of sub questions: What are the consequences of a decision that the directive is disproportionate?[2070] Also, could alternative transactions systems perhaps offer



2069 See particularly the first and fourteenth concerns discussed in Chapter IX.
2070 This research question was answered in Chapter IX.

enhanced protection to users, in order to shield them from disproportionate interference?[2071]

The CJEU is exclusively competent to rule on the proportionality of a European directive. In the event that the Anti-money laundering Directive is challenged before the Court, and if the CJEU agrees with the assessment made in this thesis, the Court will invalidate the Anti-money laundering Directive. The invalidation of the Directive would not automatically cause the invalidation of national anti-money laundering legislation; this task would be left to national courts and perhaps to some extent to the ECtHR. The anti-money laundering measures would have to be redrafted with the consideration due to the proper respect for human rights. This would essentially cause a step back to the warrant-system, according to which law enforcement authorities must identify a suspect and obtain a judicial authorisation for the access to certain identified sets of data from certain identified banking customers. This obligation to obtain a warrant would grant data subjects the higher level of protection of judicial review. The quick-freeze system may also be explored as a potential approach in order to ensure the retention of certain data sets.

However, as the CJEU is thus exclusively competent to assess the proportionality of the Directive, and as a procedure before the CJEU is time-consuming, some individuals may consider alternative transactions systems as an avenue for financial transactions, granting them additional privacy compared to the conventional banking sector.

However, as has been shown, the degree of privacy granted by alternative transactions systems is rather uncertain. In addition, the nearly universal application of the conventional banking system to all financial aspects of society in Europe makes it nearly impossible for most members of this society to avoid it. Therefore, alternative transaction systems may perhaps serve as a way to avoid some aspects of the anti-money laundering measures, but they do not present a viable alternative for most Europeans.

It has been shown above that the European anti-money laundering framework is ill-equipped to cover alternative transaction systems. The hope that the two

2071 This research question was answered in Chapter IX.

alternative systems may afford enhanced privacy is based on this incomplete coverage of the systems by the measures of the Anti-money laundering Directive. In virtual currencies, this hope is based on the fact that there is no central authority monitoring transactions on the system. As the user needs not identify him- or herself officially, it is sometimes assumed that the system is anonymous. This is not the case, however, as the transaction history of all users, including the pseudonym under which the user appears, is visible to anyone. In some cases, attackers may link information in such a way as to be able to identify users, thereby potentially revealing that user's entire transaction history. Indeed, users not particularly versed in the use of virtual currency systems are at a high risk of being identified. Virtual currency systems therefore do not offer a solution for increased privacy compared to the conventional banking sector.

In alternative transactions systems, the belief that additional privacy may be afforded to users is based on the fact that hawaladars often operate underground and are unlikely to report suspicious transactions. However, the fact that hawaladars operate underground also means that they are at risk of being targeted by the authorities when their activities are detected. In addition, Hawala is not an anonymous transaction system, and the wide-spread belief that hawaladars do not keep transaction records has been disproven repeatedly. Indeed, just as in virtual currencies, linking of information and a skilful police operation will likely reveal much information on users.[2072] Therefore, in the event of a hawaladar's being targeted by the authorities, transaction records are likely to be seized, creating additional risks for the customers. Hawala therefore also does not offer a viable alternative to the conventional banking system.

**v. A Holistic Approach**

This thesis applies the proportionality test to asssess the legality of the Anti-money laundering Directive. However, a careful examination of the proportionality test shows one serious shortcoming of the test: it can only be applied to one legal instrument or measure at a time, and that only after a lengthy legal procedure. It does not necessarily allow for the assessment of the cumulative effect of two or more measures. It is the cumulative effect, however, which will often have a particularly negative effect on the privacy of individuals.



2072 See in this context both Chapters VI and VII as well as conclusion (3) discussed below.

Against this background, Chapter X of this thesis begins the discussion of the question whether the approach currently applied to the review of the legality of surveillance measures and other intrusions into the privacy of the population is an adequate mechanism for the protection of the essence of the rights to privacy and data protection. It is clear that the mechanisms for the protection of the rights to privacy and personal data are not suitable to protect data subjects from dangers presented by Big Data projects,[2073] mass surveillance, and cleverly drafted legislation.

A holistic view of the entire landscape of the surveillance measures with which a data subject is confronted is therefore indispensable in order to ensure the proper protection of the rights of the data subject and preventing the gradual hollowing-out of the rights to privacy and data projection by the multitude of existing interferences. While each interference with the rights of the data subject may be justified and proportionate when viewed individually, the combination of these measures is well capable of interfering with the essence of the rights to privacy and data protection. The lack of meaningful protection against this danger is intolerable and should be remedied on the European level without delay. In this thesis, one possible approach has been outlined, but naturally, different approaches are also thinkable and may be viable. Further research into this direction is urgently needed.

## b. Conclusions and Recommendations

Based on the foregoing, the following five conclusions can be drawn:

***(1) The Sweeping Scope of the Anti-money laundering Measures is Incompatible with Privacy and Data Protection.***

The first and main conclusion that can be drawn based on the foregoing research is that the anti-money laundering measures collide with the proper protection of the human rights to privacy and data protection.[2074] The measures of the Directive are so far-reaching that they must be considered to be incompatible with these

2073 Goldschmidt/Bunk (2016), p. 464 f.; Rubinstein (2013), p. 76 ff.

2074 This conclusion was reached in Chapter IX, based on the assessment of the proportionality of the Anti-money laundering Directive conducted in Chapter IX.

two rights. Indeed, the terms of the Directive utterly fail to design the anti-money laundering measures in a way which is compatible with the human rights of the customers. The scope of the anti-money laundering Directive is comprehensive, establishing an intricate system of surveillance which does not contain any meaningful exceptions for persons or categories of data, and does not include meaningful safeguards for persons whose activities are covered by professional secrecy. The duty of obliged entities to identify customers is comprehensive: the system does not allow for options for anonymous transactions. The duty of obliged entities to report suspicious transactions is also connected to a number of shortcomings. The Directive speaks of suspicious transactions without defining this term, leading to a considerable lack of transparency. The continual surveillance of transactions raises questions connected to the presumption of innocence and the freedom to conduct a business. Importantly, there are no safeguards to protect sensitive personal data from disproportionate or illegitimate processing. A third duty falling on obliged entities is to report suspicious transactions, and to comply with requests for information by Financial Intelligence Units. This obligation is, however, not safeguarded by judicial oversight or other mechanisms to ensure that data is not processed contrary to the applicable legal norms. Furthermore, data subjects are not notified of their data being forwarded to the FIU. This lack of notification aggravates the intransparency of the situation, and makes the exercise of the rights of data subjects very difficult for customers. The fourth duty with which obliged entities must comply is to retain information for five years after the business relationship with the customer. This retention period is excessively long, particularly as it is not supported by meaningful explicitly codified data protection standards. Furthermore, the retained data is accessible to tax authorities, adding further to the lack of transparency for data subjects. This access by another authority than the FIU, and for another purpose than the fight against money laundering or terrorist financing leads to a situation in which the principle of purpose limitation is not properly respected.

Based on all of these seventeen considerations, particularly on the lack meaningful safeguards for personal data and sensitive data, the sweeping scope of the surveillance and the intransparency of the system, and the lack of respect for the rule of law, it is argued that the Directive does not respect the principle of proportionality, and is therefore incompatible with the rights to privacy and data protection.

Based on the foregoing, the author's first recommendation is that the Anti-money laundering Directive is challenged before the CJEU. It can be expected that in its judgement, the CJEU would not only clear away the measures it considers disproportionate, but that it would also add recommendations and guidelines of its own with which the lawmaker should comply in order to be sure that a future Anti-money laundering Directive would be considered proportionate.

In the second place, the author would recommend a halt to the negotiations concerning the fifth Anti-money laundering Directive. The lawmaker should take the serious concerns raised about the Anti-money laundering Directive outlined in this thesis into consideration and alleviate them. In order to ensure that the fifth Anti-money laundering Directive will be free of serious shortcomings, the CJEU may be asked for its opinion on the draft of the fifth Anti-money laundering Directive before it is passed into law. In any case, the law making procedure already underway should be redirected into a more open discussion on the future of anti-money laundering measures in Europe, in order to design a framework properly in line with human rights.[2075] An invalidation of the Directive currently in force would be beneficial to the law-making procedure, as it would not only create a sense of urgency, but also convey a clearer understanding of the importance of the principle of proportionality in this context.

Thirdly, it is necessary that access to the personal data of customers of obliged entities is only granted to the authortities in the presence of an authorisation. This authorisation may be a judicial warrant. The system of demanding that obliged entities forward all relevant information to the FIU, and that obliged entities comply with all requests for information from the FIU, cannot be maintained. Judicial oversight would offer the most meaningful protection of personal data against unauthorised access.

In the fourth place, the author recommends curbing the influence of international anti-money laundering expert groups, institutions, task forces, and other instruments, unless those entities unambiguously profess their commitment to human rights. International treaties and conventions concerning money laundering and terrorist financing which have already been concluded should not

2075 See also Article 29 Working Party Opinion 14/2011, p. 9: the Article 29 Working Party has made a similar recommendation back in 2011.

be applied unless their compatibility with human rights has been affirmed, for instance by the CJEU.

***(2) There is Insufficient Regard for Privacy and Identity Issues in Financial Transactions.***

The second conclusion that can be drawn is that the connection between financial transactions and privacy and identity is largely overlooked by the regulator.[2076] The impact of the anti-money laundering measures on privacy and identity is strong in several ways. In the first place, the measures do not allow for anonymous use of financial services, to the detriment of meaningful protection of customer privacy. Every member of society must have access to financial services, but under the framework currently in place, one must give up one's privacy in order to make use of these services. In the second place, and closely related, a customer's transaction record is so rich in personal information that based on the records, detailed conclusions can be drawn on the customer's private life, including on sensitive areas thereof. The lawmaker has fallen short of his obligation to include meaningful safeguards. In the third place, a customer's choice for an alternative transaction system is strongly influenced by considerations of identity. For instance, legitimate users of the Hawala system are connected to this transaction system though their cultural identity and often for religious reasons.

Furthermore, the absence of options for anonymity should be reconsidered. Anonymity is perhaps the best means to protect the privacy and identity of individuals. Where an individual is not identified, the threats to his or her privacy are significantly limited compared to where he or she is identified. Anonymity therefore facilitates the exercise of the personal freedom of an individual and the free development of his or her personality. Anonymity grants an individual spaces in which to develop unobservedly and undisturbedly.

However, the constant identification of individuals diminishes the spaces in which an individual may be anonymous. The fact that individuals are identified at so many junctures leads to a situation in which there are increasing options



2076 This conclusion was reached in Chapter VII, primarily based on the discussion of identity in Chapter VI, the discussion of the potential benefit of options of anonymity in Chapter VII, the connection between privacy and identity in these two chapters, and to some extent on the assessment of the Anti-money laundering Directive, particularly the discussion of the first, third, and fifth concerns in Chapter IX.

for the linking of information. The increasing availability of information on each individual makes it potentially easier to link previously anonymous information to an identity. Therefore, the lack of anonymity in some areas makes it increasingly difficult for individuals to achieve anonymity in others. Therefore, adding a right not to be identified to the rights of data subjects may allow individuals to limit the spaces in which they are identified in order to be able to carve out spaces for themselves in which they are not identified and therefore able to exercise their freedoms and develop in peace.

Based on the foregoing, the author recommends that the framework under which financial services are currently offered is redesigned with regard to the proper protection of the customers' privacy and identity. The European lawmaker will want to integrate the recommendations made to this effect by the various authorities in the field of data protection, particularly by the Article 29 Working Party and by the European Data Protection Supervisor.[2077]

Secondly, options for a strengthened protection of the identity of individuals should be explored. Anonymity is only one way in which such a strengthened protection may be offered, but it is a potent one, particularly in an online context. Rather than a right to anonymity, adding a right of individuals not to be identified is recommended. Such a right would allow a limit to the situations in which an individual is identified, thereby facilitating the privacy and anonymity of individuals in other areas.

***(3) Alternative Transactions Systems do not Provide Increased Privacy to Users.***
The third conclusion is that alternative transactions systems do not provide for a more privacy-friendly option for financial transactions than the conventional banking sector is.[2078] Although they are often characterised as anonymous and opaque, these characterisations cannot be sustained upon a closer inquiry. Indeed,

2077 This concerns particularly EDPS Opinion 1/17 and the Article 29 Working Party Opinions 14/2011 on the anti-money laundering measures.
2078 This conclusion was reached in Chapter IX, section (j), where the question whether alternative transaction systems provide increasing privacy to users was discussed. This discussion is based on the remarks made and explanations given in Chapter III on the functioning of alternative transaction system, Chapter IV on how transaction systems are not properly covered by the Directive, and VII, on how those transaction systems are not anonymous, but may reveal rather much information on customers.

the hasty tag of anonymity is generally based on an insufficient understanding of both the system in question and the concept of anonymity.

In reality, both systems are supported by extensive records. It is true that there is no central authority monitoring transactions on the virtual currency system, and that therefore, the system itself falls out of the scope of the Anti-money laundering Directive. As the user needs not identify him- or herself to a central authority, it is sometimes assumed that the system is anonymous. This is not the case, however. The transaction history of all users, who are identified by a pseudonym when they use the system, is visible to anyone. This applies to law enforcement authorities as well as to other interested parties: An attacker may link information in such a way as to be able to identify users. When this is done successfully, the user's entire transaction history is at risk of being revealed. Particularly users, who are not experienced in the use of virtual currency systems are at risk of being identified by an attacker. Virtual currency systems therefore do not offer a solution for increased privacy compared to the conventional banking sector.

For alternative transactions systems, the situation is similar. It may be supposed that informal value transfer services may offer enhanced privacy, based on the fact that hawaladars often operate underground and are unlikely to report users and transactions to the FIU. However, the very fact that hawaladars operate underground also entails a risk of being targeted by the authorities when their activities are detected. Contrary to wide-spread belief, Hawala is not an anonymous transaction system, and hawaladars do keep transaction records. These transaction records may potentially reveal much information on users. This is particularly a risk in the event of a hawaladar's records being seized by the authorities. Hawala therefore also does not offer a viable alternative to the conventional banking system.

The author recommends therefore that the attitude of regulators towards alternative systems for financial transactions is changed to a more positive approach. Much of the regulation of virtual currency and Hawala currently in place or proposed appears to be based on an incomplete understanding of the systems. However, the two systems virtual currencies and informal value transfer services both cater to an existing legitimate need in the population, and should be allowed space and freedom to flourish and grow in order to be able to meet this demand.[2079]

2079 Raman (2013), p. 70.

***(4) The Proportionality Assessment is Currently the Most Relevant Test, but it has Significant Weaknesses.***

The fourth conclusion resulting from this thesis is that the principle of proportionality is an important tool for the assessment of the compatibility of a certain measure with human rights.[2080] Indeed, it is the only substantial test by which this compatibility can be confirmed or denied, due to it being the test applied by the CJEU and the ECtHR.

However, the principle of proportionality is also encumbered by two significant, closely related weaknesses. Assessing the proportionality of a legal measure is in principle left up to the law-maker. The regulator, however, has shown in the past a marked disregard for the careful application of this principle. A second evaluation of the proportionality of a given legal measure is therefore often necessary, but on the European level it can only be undertaken by the CJEU upon a challenge to a certain legal act, which requires a lengthy and often costly procedure. Therefore, the weaknesses of the principle of proportionality in its current implementation are, firstly, that it is in practice largely left up to the courts which can only rule on concrete challenges, and secondly, that such a challenge can only be directed against individual legal measures. The combination of these obstacles to a proportionality review results in great difficulties for the civil population to protect their rights to privacy and data protection against the law-maker. Successful challenges by NGOs such as *Digital Rights Ireland* and individuals such as *Max Schrems* are rather rare exceptions.

Based on these observations, the author recommends in the first place a commitment to a higher regard for proportionality in the law-making procedure. In particular, new and existing legal measures involving data processing must be tested more carefully as to their compatibility with the human rights to privacy and data protection. Legal acts which are manifestly incompatible with these rights, such as the Data retention Directive or, as is argued in this thesis, the Anti-money laundering Directive, should not be passed into law in the first place.

2080 This conclusion was reached in Chapter X, where the shortcoming of the proportionality test, namely that it only allows for the assessment of a specific measure, and that only after a rather lengthy legal procedure, was discussed. The proportionality test was discussed in detail in Chapter VIII, and applied in Chapter IX to the Anti-money laundering Directive.

In addition, the example of the challenge of the Data retention Directive by *Digital Rights Ireland* and the group of over 11 thousand individuals around *Michael Seitlinger* and *Christof Tschohl* should be perceived as a valuable contribution to political participation and public discourse, and understood to express a desire of higher standards for privacy and data protection in the population. The author would therefore secondly recommend to consider making the CJEU more accessible to such groups of individuals, NGOs, and other interest groups, so that they can express their dissatisfaction with certain legal measures by challenging them more easily before the Court.

***(5) The Proper Protection of the Essence of Privacy Requires a New Test.***

The fifth and final conclusion which can be reached based on the research recorded in this thesis is that the principle of proportionality does not suffice to ensure adequate protection of the rights to privacy and data protection in the future, particularly against measures of mass surveillance.[2081] This conclusion is based on the weaknesses with the proportionality test mentioned above. While the application of the recommendations connected to conclusion four can improve the effectiveness of the principle of proportionality, it must be questioned whether the principle itself must not be fundamentally reassessed.

A viable approach to ensure the respect for the essence of the rights to privacy and data protection may be to apply a holistic approach.[2082] The application of such an approach would demand that a designated authority keeps close watch over changes to the landscape of surveillance. This would mean that all legal measures impacting the privacy and personal data of the population must be registered, indexed, and assessed as to the seriousness of the interference with the rights to privacy and data protection caused by each measure. This would include in the first place legal measures ordering data processing operations, such as mass surveillance programmes, in the second place legal measures granting permission to public and private entities to collect and process personal data, and thirdly, gaps in the data protection framework due to which the rights of all or parts of the population are not sufficiently protected from interferences. This last point would include particularly the data collection and acquisitiveness of personal data by



2081 This conclusion was reached in Chapter X, where a holistic approach to the review of the impact of measures on the privacy and personal data of individuals was proposed. This proposal is based on the shortcomings defined earlier, which are the subject of conclusion (4).

2082 BVerfG, 1 BvR 256/08 [2010], paragraph 218. See particularly Chapter X.

private entities, big data and open data applications, and miscellaneous difficulties encountered by data subjects, such as difficulties in asserting their rights against controllers.

This registration of interferences would have the secondary effect of informing the public about such measures and thereby facilitating public discourse, and making it easier for interested parties to identify disproportionate interferences such as the data retention obligations and the anti-money laundering measures. Primarily, however, the survey of the landscape of surveillance should be used to assess the cumulative impact of all those interferences with the human rights to privacy and data protection of the population. The necessity for such a holistic approach lies in the connection between privacy and human dignity, and in the importance of privacy and data protection for the uninhibited exercise of other human rights of the data subject. It is generally accepted that the right to privacy is one of the most important pillars for a functioning democracy.[2083] A holistic approach to privacy would be an important safeguard against this right slowly being hollowed out by the cumulative effect of an unprecedented amount of legal data processing operations in combination with weak mechanisms for the protection of personal data and the privacy of the individual.

The author therefore finally recommends that the lawmaker embraces a holistic approach to the right to privacy. Only when viewed in combination, the impact of mass surveillance and the cumulative impact of all the interferences with privacy can be assessed. It must then be assessed whether the cumulative level of interferences with privacy and data protection can be borne by society, or if the level has become critical. The tacit implication of the adoption of such an approach would also be that surveillance measures must sometimes be rolled back before new measures can be introduced. Such a standard would be somewhat difficult to implement, but its potential benefit in terms of an increased standard of protection of the rights to privacy and data protection should not be underestimated.

2083 See decisively BVerfG, 1 BvR 256/08 [2010], paragraph 218. See also CJEU Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* [2016], paragraph 101. See also decicively Böhme-Neßler (2016), p. 5 f.; Tinnefeld (2007), p. 628 f.; Maras (2012), p. 72 f.; Hirsch (2008b), p. 89.

## c. Developments in this Field of Research

### i. Recent Developments

During the time in which this research was conducted, the legislation has developed rapidly. The last four years have seen far-reaching upheavals. Since 2013, the European legislator has moved from the third Anti-money laundering Directive via the fourth to proposing a fifth Directive. The European legislator thus acts very quickly in updating the legal framework. Member States follow suit: at the time of writing the national law in all Member States has just been updated to comply with the fourth Anti-money laundering Directive, and legislators have to take into account that the text of this fourth Directive may at short notice be amended by the fifth Anti-money laundering Directive, which is currently still going through the law-making process on the European level. The measures contained in these Directives have been continually increased in severity, demanding ever increasing vigilance of obliged parties in fields identified as particularly vulnerable to money laundering by the lawmaker. Virtual currencies are the latest addition to the number of covered structures.

The legislation is however not the only aspect of this research that has developed rapidly. The general public has steadily become more aware of virtual currencies, as media coverage increased and information became more accessible. At the same time, both the number of users and the number of businesses accepting virtual currencies for payments appear to increase steadily. Several major events agitated this development, beginning with an immense rise in the value of Bitcoin, rising to a value of over 7,500 US Dollar in early November 2017. This multiplies the value of an early peak value of over 1000 US Dollar in November 2013. Events began unfolding rapidly around this time, with the closing of Mt. Gox, the biggest exchange for virtual currencies at that time,[2084] the media-intensive take-down of the market place Silk Road[2085] and the subsequent trial of its operator, the immense ongoing hype around the blockchain technology underlying the major decentral virtual currencies,[2086] and finally the latest amendment to the anti-money laundering framework to bring virtual currencies under the umbrella of financial regulation. In contrast, the Hawala network has remained in comfortable

2084 Anderson (2014), p. 430.
2085 Raman (2013), p. 67 f.; Dowd (2014), p. 70 ff.
2086 Simmchen (2017), p. 162.

obscurity, still largely unknown to the general public, and undisturbed by targeted legislative action.

Simultaneously, the rights to privacy and data protection have received a significant share of the public attention, and a heightened level of protection by the CJEU's case law, supported by the highest courts in many Member States, particularly through the series of cases on data retention. A chain of case law is currently observable on the level of the CJEU, in which the Court steadily increases the standard of protection of the rights to privacy and data protection by landmark judgments in that area, with the *Digital Rights Ireland, Google Spain, Schrems*, and most recently *Tele2 Sverige* cases.[2087] In each judgment the CJEU took the opportunity to emphasise the importance of the rights to privacy and data protection and the principle of proportionality. Particularly the two cases *Digital Rights Ireland* and *Tele2 Sverige,* decided on European level, could potentially act as a guidance towards a higher protection of privacy also in other areas of law, such as described here for the complex of anti-money laundering legislation.

This increased judicial protection coincided with the adoption of the GDPR as the new main framework for European data protection law. The GDPR replaces the current data protection framework contained in Directive 95/46/EC, which was in need of an update to make it fit for new challenges of data processing. The GDPR was adopted on April 27th, 2016, and is scheduled to enter into force on May 25th, 2018. The impact of the new regulation is naturally not yet estimable, but it can safely be said that the developments in the field of data protection are far from finished.

**ii. Upcoming Developments**

There are several areas of research covered in this thesis in which major developments can be expected in the next few years. In the first place, major changes to the legal framework are being implemented at the moment. The GDPR has been passed and will shortly be directly applicable, bringing with it changes in the national legal systems throughout Europe. How this legal development will impact the rights to privacy and data protection in practice is not yet entirely foreseeable, making the mere observation of this development an interesting exercise. In the second place, the anti-money laundering rules are also going to go

2087 See also Chapter VIII above.

through major changes in the upcoming period of time. The fourth Anti-money laundering Directive entered into force on 26 June 2017, with a fifth Directive expected to follow closely on its heels. These new Directives essentially tighten the existing framework, so the tangible impact of the Directives can be expected to be slightly smaller in scope than that of the GDPR. However, two Directives tightening the framework in such close succession will certainly cause major changes in the application of anti-money laundering rules throughout Europe.

Connected to the legal development is the development in the case law concerning those laws. It will be observed with much interest whether the CJEU continues to hand down decisions in favour of enhanced protection of privacy and data protection rights in as rapid a succession as it did in the past few years. There are several interesting cases pending before the CJEU as well as before the ECtHR, to be decided in the near future.

In addition, the development of virtual currencies is also progressing at a rapid pace. Not only have a number of successful alternatives to the dominant first mover Bitcoin been introduced, such as *Ripple* and *Ethereum*, both of which offer potentially viable alternatives to perceived weaknesses in the Bitcoin architecture. Also, the blockchain technology and the concept of virtual currencies is slowly arriving in the mainstream. This brings with it a call for legal recognition of this technology, which is being heard by the legislator, and a progression towards safer and more varied applications. It can be expected that the blockchain technology is going to find application in different branches of industry and business, and that virtual currencies are shortly going to be considered an alternative transaction system potentially usable by anyone. If the use of virtual currencies can be made safer and more convenient to use for individuals without any special technical talents, they will soon be regarded as an option as suitable as is, for example, *paypal*.

In contrast, as has already been shown above, Hawala is remaining comfortably undisturbed. The initial crackdown on terrorist financing after the events of 11 September 2001 specifically targeted Hawala, to little long-term avail. The dust of this attack on the Hawala system is slowly settling. The second wave of action against terrorist financing is ongoing, with the Commission's Action Plan and a number of new directives, but in none of those instruments is Hawala explicitly mentioned or expected to play a more significant role. It can therefore be expected

that Hawaladars will also in the future be able to continue to carry out their businesses without major interferences.

None of the upcoming developments, however, is likely to have a significant impact on the conclusions reached in this thesis. This thesis was drafted in such a way as to cover all decentralised virtual currencies rather than only Bitcoin, so that the conclusions of this thesis will still apply in case Bitcoin is replaced as the virtual currency with the largest area of application. It is not likely that changes in the Hawala system are going to take place. The (foreseeable) upcoming changes in the legal situation are also already discussed in this thesis. The proposed amendments to the fifth Anti-money laundering Directive are discussed in appropriate places throughout this thesis. Indeed, the only unpredictable element is the case law. It is unlikely that the CJEU will make any radical changes to the course it has adopted in cases on privacy and data protection. This presumed constancy is the reason why the assessment of the proportionality of the Anti-money laundering Directive was assessed based on the existing case law of the Court. Naturally, it can never be entirely ruled out that the Court will deviate from existing case law in the future. However, based on the existing case law, one may trust in the continual commitment of the CJEU to a high level of protection for privacy and personal data.

### iii. Concluding Remarks: Further Research

These developments also highlight some areas in which further research is needed. This thesis will therefore conclude with a few selected areas in which more research is needed. It may be hoped that this field attracts researchers who are willing to immerse themselves in the subject matter and follow any of the lines outlined in these concluding paragraphs, or in any other point in this thesis.

In the first place, the amended Directives[2088] must, naturally, be tested as to their compliance with human rights and the principle of proportionality. It has already been mentioned in earlier chapters that the problems of the fourth Anti-money

2088 This concerns for instance Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21, and Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, OJ L 342, 16.12.2016, p. 1–3. Both of these instruments have been briefly discussed in Chapter IX, but not individually tested as to their proportionality.

laundering Directive are not alleviated by the proposed fifth Directive, but instead rather aggravated. When this proposed fifth Directive is finally passed, its final text must be examined and tested carefully against human rights concerns.

In the event that the disproportionality of the anti-money laundering legislation is confirmed by the CJEU or otherwise recognised by the lawmaker, the rules should be re-examined carefully in order to return to a balance between the interest in the fight against serious crime on the one hand and the interest in the protection of privacy and data protection on the other hand. The design of suitable rules replacing the current anti-money laundering framework will be very difficult in the current political climate, but certainly not impossible. Some leads have been outlined in Chapter IX of this thesis, but a mature draft for new legislation requires extensive research and stakeholder dialogue.

In addition, more research is needed concerning alternative transaction systems. Not only has the work of writing and rewriting legislation governing virtual currencies only just begun, this legislation must be designed carefully in order to cover virtual currencies in a sensible and effective way. A better understanding of virtual currencies and the underlying technical architecture on the part of the legislator is indispensable if this transition is to be successful. Such an understanding requires extensive further research into the inner workings of both the virtual currency architecture itself and the community of users.

Similarly, it would be welcomed if Hawala could be brought under sensible legislation, respecting the legitimate need for those services in some segments of the society. In order for such sensibility to be achieved, Hawala must, in the minds of legislators as well as the general public, be divorced from terrorism and terrorist financing. Such a reversal of an accepted stereotype will demand much work, including extensive research along the same lines as that proposed for virtual currencies.

Naturally, the research into privacy and proportionality is also not at an end. The ongoing and upcoming developments outlined above in the legislation on privacy and data protection will give rise to both a need to revisit earlier research and a large amount of new research leads. Similarly, each of the landmark decisions of

both the CJEU and the ECtHR have added fuel to an ongoing discussion of the principle of proportionality and its content.

In addition, the output of the discussion and research into the principle of proportionality may lead to other research as that conducted in the present thesis, in which the lessons learned in, among other things, the case law of the CJEU, are applied to other legislation in order to test their legality. The increasing amount of legislation containing measures that interfere with the rights to privacy and data protection provides researchers with plenty of material in that regard.

Finally, and in connection to the above, more research into the concept of the essence of a right under the Charter of Fundamental Rights and the viability of a holistic approach would be highly desirable. Several leads have been presented and outlined in the previous Chapter X, which may be explored with benefit. The question whether a holistic approach to the essence of the right to privacy may be a viable option for the improved protection of privacy and personal data must especially be further explored, and may deliver an interesting topic for several future research projects.

# PART D

## ANNEXES

# I

# Register of Case Law

## a. ECtHR

*Case of Lawless v. Ireland* (No. 3), Judgment of 1 July 1961, Application no 332/57, ECLI:CE:ECHR:1961:0701JUD000033257.

*Case of G.W. v. Federal Republic of Germany*, Decision of 4 October 1962, Application no. 1307/61, ECLI:CE:ECHR:1962:1004DEC000130761

*Case of Handyside v. the United Kingdom*, Judgment of 7 December 1976, Application no. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372

*Case of Klass and Others v. Germany,* Judgment of 6 September 1978, Application no. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971

*Case of Sporrong and Lönnroth v. Sweden*, Judgment of 23 September 1982, Application nos. 7151/75 and 7152/75, ECLI:CE:ECHR:1982:0923JUD000715175

*Case of X. v. Belgium*, Decision of 07 December 1982 on the admissibility of the application, Application no. 9804/82, ECLI:CE:ECHR:1982:1207DEC000980482

*Case of Malone v. the United Kingdom*, Judgment of 2. August 1984, Application no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179.

*Case of Leander v. Sweden,* Judgment of 26 March 1987, Application no. 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881

*Case of Funke v. France*, Judgment of 25 February 1993, Application no. 10828/84, ECLI:CE:ECHR:1993:0225JUD001082884

*Case of Crémieux v. France*, Judgment of 25 February 1993, Application no. 11471/85, ECLI:CE:ECHR:1993:0225JUD001147185.

*Case of Miailhe v. France*, Judgment of 25 February 1993, Application no. 12661/87, ECLI:CE:ECHR:1993:0225JUD001266187.

*Case of Murray v. the United Kingdom*, Judgment of 28 October 1994, Application no. 14310/88, ECLI:CE:ECHR:1994:1028JUD001431088.

*Case of Amann v. Switzerland,* Judgment of 16 February 2000, Application no. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895

*Case of Société Colas Est and others v. France*, Judgment of 16 April 2002, Application no. 37971/97, ECLI:CE:ECHR:2002:0416JUD003797197

*Case of Wypych v. Poland*, Decision of 25 October 2005 on the admissibility of the application, Application no. 2428/05, ECLI:CE:ECHR:2005:1025DEC000242805

*Case of Segerstedt-Wiberg and Others v. Sweden,* Judgment of 6 June 2006, Application no. 62332/00, ECLI:CE:ECHR:2006:0606JUD006233200

*Case of S. and Marper v. The United Kingdom,* Judgment of 4 December 2008, Applications nos. 30562/04 and 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204

*Case of Uzun v. Germany,* Judgment of 2 September 2010, Application no. 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305

*Case of Köpke v. Germany,* Decision as to the Admissibility of the Application taken on 5 October 2010, Application no. 420/07, ECLI:CE:ECHR:2010:1005DEC000042007

*Case of Bernh Larsen Holding AS and others v. Norway*, Judgment of 14 March 2013, Application no. 24117/08, ECLI:CE:ECHR:2013:0314JUD002411708.

*Case of Roman Zakharov v. Russia,* Judgment of 4 December 2015, Application no. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306

*Case of Szabó and Vissy v. Hungary,* Judgment of 12 January 2016, Application no. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814.

*Case of K.S. and M.S. v. Germany*, Judgment of 6 October 2016, Application no. 33696/11, ECLI:CE:ECHR:2016:1006JUD003369611

*Case of Vanja Ćalović v. Montenegro,* Application no. 18667/11 lodged on 14 March 2011, Communicated Case.

*Case of Big Brother Watch and Others v. the United Kingdom*, Application no. 58170/13, lodged on 4 September 2013, Communicated Case.

## b. CJEU

*Case C-6/64:* Judgment of the Court of 15 July 1964, *Flaminio Costa v E.N.E.L.* Case 6-64. ECLI identifier: ECLI:EU:C:1964:66

*Case C-11/70*: Judgment of the Court of 17 December 1970, Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel. ECLI identifier: ECLI:EU:C:1970:114.

*Case C-145/83*: Judgment of the Court of 7 November 1985, Stanley George Adams v Commission of the European Communities. ECLI identifier: ECLI:EU:C:1985:448.

*Case C-331/88*: Judgment of the Court (Fifth Chamber) of 13 November 1990, The Queen v Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa and others. ECLI identifier: ECLI:EU:C:1990:391

*Opinion 2/94:* Opinion of the Court of 28 March 1996, Opinion pursuant to Article 228 of the EC Treaty. Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms. ECLI identifier: ECLI:EU:C:1996:140

*Joined cases C-465/00, C-138/01 and C-139/01:* Judgment of the Court of 20 May 2003, Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk. ECLI identifier: ECLI:EU:C:2003:294

*Case C-101/01:* Judgment of the Court of 6 November 2003, Criminal proceedings against Bodil Lindqvist. ECLI identifier: ECLI:EU:C:2003:596

*Case C-189/01:* Judgment of the Court of 12 July 2001, H. Jippes, Afdeling Groningen van de Nederlandse Vereniging tot Bescherming van Dieren and Afdeling Assen en omstreken van de Nederlandse Vereniging tot Bescherming van Dieren v Minister van Landbouw, Natuurbeheer en Visserij. ECLI identifier: ECLI:EU:C:2001:420

*Case C-491/01*: Judgment of the Court of 10 December 2002, The Queen v Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd. ECLI identifier: ECLI:EU:C:2002:741

*Case T-47/03:* Judgment of the Court of First Instance (Second Chamber) of 11 July 2007, Jose Maria Sison v Council of the European Union. ECLI identifier: ECLI:EU:T:2007:207.

*Joined cases C-453/03, C-11/04, C-12/04 and C-194/04:* Judgment of the Court (Grand Chamber) of 6 December 2005, The Queen, on the application of ABNA Ltd and Others v Secretary of State for Health and Food Standards Agency (C-453/03), Fratelli Martini & C. SpA and Cargill Srl v Ministero delle Politiche Agricole e Forestali and Others (C-11/04), Ferrari Mangimi Srl and Associazione nazionale tra i produttori di alimenti zootecnici (Assalzoo) v Ministero delle Politiche Agricole e Forestali and Others (C-12/04) and Nederlandse Vereniging Diervoederindustrie (Nevedi) v Productschap Diervoeder (C-194/04). ECLI identifier: ECLI:EU:C:2005:741

*Joined cases C-317/04 and C-318/04.:* Judgment of the Court (Grand Chamber) of 30 May 2006, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04). ECLI identifier: ECLI:EU:C:2006:346

*Case C-305/05:* Judgment of the Court (Grand Chamber) of 26 June 2007, Ordre des barreaux francophones et germanophone and Others v Conseil des ministres. ECLI identifier: ECLI:EU:C:2007:383

*Case C-275/06:* Judgment of the Court (Grand Chamber) of 29 January 2008, Productores de Música de España (Promusicae) v Telefónica de España SAU. ECLI identifier: ECLI:EU:C:2008:54

*Case C-301/06:* Judgment of the Court (Grand Chamber) of 10 February 2009, Ireland v European Parliament and Council of the European Union. ECLI identifier: ECLI:EU:C:2009:68

*Case C-28/08 P:* Judgment of the Court (Grand Chamber) of 29 June 2010, European Commission v The Bavarian Lager Co. Ltd. ECLI identifier: ECLI:EU:C:2010:378

*Case C-402/05 P:* Judgment of the Court (Grand Chamber) of 3 September 2008, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, ECLI identifier: ECLI:EU:C:2008:461.

*Case T-341/07:* Judgment of the General Court (Second Chamber, extended composition) of 23 November 2011, Jose Maria Sison v Council of the European Union. ECLI identifier: ECLI:EU:T:2011:687

*Joined cases C-92/09 and C-93/09:* Judgment of the Court (Grand Chamber) of 9 November 2010, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. ECLI identifier: ECLI:EU:C:2010:662

*Case C-343/09:* Judgment of the Court (Fourth Chamber) of 8 July 2010, Afton Chemical Limited v Secretary of State for Transport. ECLI identifier: ECLI:EU:C:2010:419

*Case C-360/10:* Judgment of the Court (Third Chamber) of 16 February 2012, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV. ECLI identifier: ECLI:EU:C:2012:85

*Case C-461/10:* Judgment of the Court (Third Chamber), 19 April 2012, Bonnier Audio AB and Others v Perfect Communication Sweden AB. ECLI identifier: ECLI:EU:C:2012:219

*Joined Cases C-581/10 and C-629/10:* Judgment of the Court (Grand Chamber), 23 October 2012, Emeka Nelson and Others v Deutsche Lufthansa AG and TUI Travel plc and Others v Civil Aviation Authority. ECLI identifier: ECLI:EU:C:2012:657

*Case C-212/11:* Judgment of the Court (Third Chamber), 25 April 2013, Jyske Bank Gibraltar Ltd v Administración del Estado. ECLI identifier: ECLI:EU:C:2013:270.

*Case C-131/12:* Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. ECLI identifier: ECLI:EU:C:2014:317

*Joined Cases C-293/12 and C-594/12:* Judgment of the Court (Grand Chamber) of 8 April 2014. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, OJ C 175, 10.6.2014, p. 6–7, ECLI identifier: ECLI:EU:C:2014:238

*Opinion 2/13:* Opinion of the Court (Full Court) of 18 December 2014, Opinion pursuant to Article 218(11) TFEU. Draft international agreement — Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms — Compatibility of the draft agreement with the EU and FEU Treaties. ECLI identifier: ECLI:EU:C:2014:2454

*Case C-580/13:* Judgment of the Court (Fourth Chamber) of 16 July 2015, Coty Germany GmbH v Stadtsparkasse Magdeburg. ECLI identifier: ECLI:EU:C:2015:485.

*Case C-201/14*: Judgment of the Court (Third Chamber) of 1 October 2015, Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others, ECLI identifier: ECLI:EU:C:2015:638.

*Case C-264/14:* Judgment of the Court (Fifth Chamber) of 22 October 2015, *Skatteverket v David Hedqvist*, ECLI identifier: ECLI:EU:C:2015:718

*Case C-362/14:* Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner. ECLI identifier: ECLI:EU:C:2015:650

*Case C-582/14:* Judgment of the Court (Second Chamber) of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI identifier: ECLI:EU:C:2016:779.

*Opinion 1/15:* Opinion of the Court (Grand Chamber) of 26 July 2017, Opinion pursuant to Article 218(11) TFEU. Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada — Appropriate legal bases — Article 16(2), point (d) of the second subparagraph of Article 82(1) and Article 87(2)(a) TFEU — Compatibility with Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union. ECLI identifier: ECLI:EU:C:2017:592.

*Joined Cases C-203/15 and C-698/15:* Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others. ECLI identifier: ECLI:EU:C:2016:970

## c. National Law

### i. Bundesverfassungsgericht

Bundesverfassungsgericht, Beschluss vom 29. Mai 1974 - Az. 2 BvL 52/71 (Solange I), BVerfGE 37, 271 – 305.

Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983 - Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil), BVerfGE 65, 1.

Bundesverfassungsgericht, Beschluss vom 22. Oktober 1986 · Az. 2 BvR 197/83 (Solange II), BVerfGE 73, 339 – 388.

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 26. April 1994 - 1 BvR 1689/88 - Rn. (1-30), BVerfGE 90, 255 – 263. ECLI:DE:BVerfG:1994:rs19940426.1bvr168988.

Bundesverfassungsgericht, Urteil des Zweiten Senats vom 05. Februar 2004 - 2 BvR 2029/01 - Rn. (1-202), BVerfGE 109, 133 – 190. ECLI:DE:BVerfG:2004:rs20040205.2bvr202901.

Bundesverfassungsgericht, Urteil des Ersten Senats vom 03. März 2004 - 1 BvR 2378/98 - Rn. (1-373), BVerfGE 109, 279 – 391. ECLI:DE:BVerfG:2004:rs20040303.1bvr237898.

Bundesverfassungsgericht, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333), BVerfGE 120, 274 – 350. ECLI:DE:BVerfG:2008:rs20080227.1bvr037007.

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 13. Juni 2007 - 1 BvR 1550/03 - Rn. (1-184), BVerfGE 118, 168 – 211. ECLI:DE:BVerfG:2007:rs20070613.1bvr155003.

Bundesverfassungsgericht, Beschluss der 2. Kammer des Zweiten Senats vom 26. Juni 2008 - 2 BvR 219/08 - Rn. (1-30). ECLI:DE:BVerfG:2008:rk20080626.2bvr021908.

Bundesverfassungsgericht, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 - Rn. (1-345), BVerfGE 125, 260 – 385. ECLI:DE:BVerfG:2010:rs20100302.1bvr025608.

Bundesverfassungsgericht, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 - Rn. (1-360), BVerfGE 141, 220 – 378. ECLI:DE:BVerfG:2016:rs20160420.1bvr096609.

**ii. UK Supreme Court**

Supreme Court of the United Kingdom, Lumsdon & Ors, R (on the application of) v Legal Services Board [2015] UKSC 41 (24 June 2015).

Supreme Court of the United Kingdom, Bank Mellat v Her Majesty's Treasury (No. 2) [2013] UKSC 39 (19 June 2013).

**iii. USA Supreme Court**

Supreme Court of the United States, decision of April 21, 1976, *United States v. Miller*, 425 U.S. 435 (1976), pp. 441-443.

Supreme Court of the United States, decision of April 19, 1995, *Joseph McIntyre, executor of estate of Margaret McIntyre, deceased, Petitioner v. Ohio Elections Commission*, on writ of certiorari to the Supreme Court of Ohio, (93-986), 514 U.S. 334 (1995).

Supreme Court of the United States, decision of January 23, 2012, United States v. Jones, 132 S.Ct. 945 (2012).

# II

# Register of Legislation

## a. International Instruments

Council of Europe Recommendation No. R(80)10 of the Committee of Ministers to Member States on Measures against the Transfer and the Safekeeping of Funds of Criminal Origin. Adopted by the Committee of Ministers on 20 June 1980 at the 321st meeting of the Ministers' Deputies.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28. January 1981 ETS No.108, entered into force 1. October 1985.

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, adopted by the United Nations Conference for the Adoption of a Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, held at Vienna from 25 November to 20 December 1988, Registration No. 27627, UN Treaty Series vol. 1582, p. 95.

Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the protection of the European Communities' financial interests. OJ C 316, 27.11.1995, p. 49–57.

International Convention for the Suppression of the Financing of Terrorism, Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999, Registration No. 38349, UN Treaty Series vol. 2178, 197.

United Nations Convention against Transnational Organized Crime and the Protocols thereto, Adopted by resolution A/RES/55/25 of 15 November 2000 at the fifty-fifth session of the General Assembly of the United Nations, Registration No. No. 39574, UN Treaty Series vol. 2225, p. 209.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 16. May 2005, CETS No.198, entered into force 1 May 2008.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union: Consolidated version of the Treaty on European Union (TEU), Consolidated version of the Treaty on the Functioning of the European Union (TFEU), Protocols, Annexes, Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, OJ C 326, 26.10.2012, p. 1–390.

Charter of Fundamental Rights of the European Union (the Charter), OJ C 326, 26.10.2012, p. 391–407.

## b. European Union Secondary Law

*Council Directive 91/308/EEC* of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, OJ L 166, 28.6.1991, p. 77–82.

*Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

*Joint action 98/733/JHA* of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union, OJ L 351, 29.12.1998, p. 1–3.

*Council Decision of 17 October 2000* concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000, p. 4–6.

*Directive 2000/31/EC* of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

*Regulation (EC) No 45/2001* of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22.

*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 - Commission Declaration, OJ L 344, 28.12.2001, p. 76–82.

*Directive 2002/92/EC* of the European Parliament and of the Council of 9 December 2002 on insurance mediation, OJ L 9, 15.1.2003, p. 3–10.

*Council Framework Decision 2002/475/JHA* of 13 June 2002 on combating terrorism, OJ L 164, 22.6.2002, p. 3–7.

*Directive 2004/39/EC* of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC, OJ L 145, 30.4.2004, p. 1–44.

*Directive 2004/48/EC* of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance), OJ L 157, 30.4.2004, p. 45–86.

*Directive 2005/60/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 (Text with EEA relevance), OJ L 309, 25.11.2005, p. 15–36.

*Regulation (EC) No 1889/2005* of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, OJ L 309, 25.11.2005, p. 9–12.

*Directive 2006/24/EC* of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

*Directive 2009/101/EC* of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (Text with EEA relevance), OJ L 258, 1.10.2009, p. 11–19

*Directive 2009/110/EC* of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance), OJ L 267, 10.10.2009, p. 7–17

*Directive 2009/138/EC* of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (Text with EEA relevance), OJ L 335, 17.12.2009, p. 1–155.

*Council Directive 2011/16/EU* of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, OJ L 64, 11.3.2011, p. 1–12.

*Directive 2013/36/EU* of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 27.6.2013, p. 338–436.

*Regulation (EU) No 575/2013* of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms

and amending Regulation (EU) No 648/2012 Text with EEA relevance, OJ L 176, 27.6.2013, p. 1–337.

*Directive 2014/42/EU* of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ L 127, 29.4.2014, p. 39–50.

*Directive 2014/92/EU* of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, OJ L 257, 28.8.2014, p. 214–246.

*Directive 2014/95/EU* of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups Text with EEA relevance, OJ L 330, 15.11.2014, p. 1–9.

*Directive (EU) 2015/849* of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117.

*Directive (EU) 2015/2366* of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127.

*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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

*Directive (EU) 2016/680* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

*Directive (EU) 2016/681* of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

*Council Directive (EU) 2016/2258* of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, OJ L 342, 16.12.2016, p. 1–3.

*Directive (EU) 2017/541* of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21.

## c. National Law

### i. Germany

Germany – Grundgesetz für die Bundesrepublik Deutschland vom 23.05.1949 (BGBl. S. 1), zuletzt geändert durch Gesetz vom 13.07.2017 (BGBl. I S. 2347) m.W.v. 20.07.2017

Germany – Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 11.06.2017 (BGBl. I S. 1612) m.W.v. 01.07.2017.

Germany – Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das durch Artikel 2 des Gesetzes vom 1. September 2016 (BGBl. I S. 3352) geändert worden ist.

**ii. The Netherlands**

The Netherlands – Wet van 21 juli 2007, houdende algemene bepalingen betreffende de toekenning, het beheer en het gebruik van het burgerservicenummer (Wet algemene bepalingen burgerservicenummer), BWBR0022428, geldend van 06-01-2014.

**iii. The United States**

The United States – The United States Constitution of 1787, in effect since March 4, 1789.

The United States – The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.), commonly referred to as Bank Secrecy Act.

The United States – The Right to Financial Privacy Act of 1978 (12 U.S.C. ch. 35, § 3401 et seq.), commonly referred to as RFPA or Financial Privacy Act.

The United States – The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Pub. L. No. 107-56, 115 Stat. 272 (2001), codified as amended in different sections of 12, 15, 18, and 31 U.S.C.), commonly referred to as (USA) Patriot Act.

# III

# Register of Abbreviations

1AMLD – the first Anti-money laundering Directive 91/308/EEC
2AMLD – the second Anti-money laundering Directive 2001/97/EC
3AMLD – the third Anti-money laundering Directive 2005/60/EC
4AMLD – the fourth Anti-money laundering Directive (EU) 2015/849
5AMLD – the proposed fifth Anti-money laundering Directive, Procedure 2016/0208/COD
AML – Anti-Money Laundering
BVerfG – the *Bundesverfassungsgericht*, the German Constitutional Court.
CFT – Countering the Financing of Terrorism
CJEU – the Court of Justice of the European Union
CRD – the Capital Requirements Directive 2013/36/EU
CRR – the Capital Requirements Regulation (EU) 575/2013
DRD – the Data Retention Directive 2006/24/EC
ECHR – the European Convention of Human Rights
ECtHR – the European Court of Human Rights
EDPS – the European Data Protection Supervisor
EU – the European Union
EUR – Euro
FATF – the Financial Action Task Force
FIU – a Financial Intelligence Unit
GBP – Great Britain Pound Sterling
GDP – Gross Domestic Product
GDPR – the General Data Protection Regulation (EU) 2016/679
NGO – a Non-governmental Organization
PEP – a Politically Exposed Person
PNR – Passenger Name Records
TEU – the Treaty on European Union
TFEU – the Treaty on the Functioning of the European Union
Tor – The Onion Router
USD – US Dollars

# IV

# Literature

All online sources last accessed 3. January 2018


Aaken, Anne van (2009), Defragmentation of Public International Law Through Interpretation: A Methodological Proposal. Indiana Journal of Global Legal Studies, Vol. 16, No. 2, Special Issue: Symposium: Global Constitutionalism – Process and Substance; Kadersteg, Switzerland, January 17-20, 2008; Guest Editors: Anne Peters and Klaus Armingeon (Summer 2009), pp. 483-512.

Abate, Constantin, Online-Durchsuchung, Quellen-Telekommunikation-süberwachung und die Tücke im Detail. Einfluss rechtlicher und technischer Entwicklungen auf verdeckte Online-Ermittlungen zur Gewährleistung der Inneren Sicherheit. In Datenschutz und Datensicherheit (DuD) 2 2011, pp. 122-125.

Abramova, Irina, Role of ethnic diasporas and migrants in the formation of conditions to finance international terrorism. In Foertsch, Volker and Lange, Klaus, Islamischer Terrorismus – Bestandsaufnahme und Bekämpfungsmöglichkeiten. Hans Seidel Stiftung, München 2005, pp. 100-111.

Adamski, Andrzej, Telecommunication Data Retention in Poland: Does the Legal Regulation Pass the Proportionality Test? In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 395-402.

Aggarwal, Reena and Demirgüç-Kunt, Asli and Martinez Peria, Maria Soledad, Do Workers' Remittances Promote Financial Development? (July 1, 2006). World Bank Policy Research Working Paper No. 3957. Available at SSRN: http://ssrn.com/abstract=923264

Ahrens, Hans-Jürgen, Das zur Zeugnisverweigerung berechtigende Bankgeheimnis contra effektive Justizgewährung im Unionsrecht. Ein zweifelhaftes Judikat des EuGH zum markenrechtlichen Auskunftsanspruch. In Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2015, pp. 1083-1085

Al-Jumaili, Diana, Stationen im Kampf gegen die Terrorismusfinanzierung. New York – Brüssel – Berlin. In Neue Juristische Online-Zeitschrift (NJOZ) 2008, pp. 188-211.

Allaire, Jeremy, Testimony of Jeremy Allaire, Chairman and CEO, Circle Internet Financial, Before the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013. In: Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf

Allen, Ernie, Testimony of Ernie Allen, President and CEO, The International Centre for Missing & Exploited Children, for the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013. In: Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf

Amendola, Sandro and Kraus, Detlef, Prüfung der Sicherheit kreditwirtschaftlicher IT-Anwendungen. In Datenschutz und Datensicherheit (DuD) 1 2015, pp. 12-15.

Amoore, Louise and De Goede, Marieke, Transactions after 9/11: the banal face of the preemptive strike. In The Transactions of the Institute of British Geographers, NS 33, 2008, pp. 173-185.

Anderson, Tracey A., Bitcoin – is it just a fad? History, current status and future of the cyber-currency revolution. In Journal of International Banking Law and Regulation 2014, 29(7), pp. 428-435.

Arendt, Hannah, The Origins of Totalitarianism. First published 1951. New Edition with added Prefaces, Harcourt New York 1973.

Arnauld, Andreas von, Der Weg zu einem „Solange I 1/2". In Europarecht (EuR) 2013, p. 236-247.

Article 29 Data Protection Working Party, Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing (WP186). Adopted on 13 June 2011.

Article 29 Data Protection Working Party, Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive (WP201), Adopted on 26 February 2013.

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

Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (WP215). Adopted on 10 April 2014.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (WP216), Adopted on 10 April 2014.

Article 29 Data Protection Working Party, Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Direcitve (WP220). Adopted on 1 August 2014.

Article 29 Data Protection Working Party, Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes (WP 230), Adopted on 4 February 2015

Article 29 Data Protection Working Party, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (WP 233), Adopted on 01 December 2015

Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP 237), Adopted on 13 April 2016.

Arzt, Gunther, 'Geldwäscherei – Eine neue Masche zwischen Hehlerei, Strafvereitelung und Begünstigung' (1990), Neue Zeitschrift für Strafrecht (NStZ) 1990, p 1-6

Bailey, Jane, Systematic government access to private-sector data in Canada. In International Data Privacy Law (IDPL), Vol. 2, No. 4, 2012, pp. 207-219.

Ballard, Lara A., The Dao of Privacy. In Masaryk University Journal of Law and Technology, Volume 7, 2013, pp. 107-176.

Bälz, Kilian, Islamische Aktienfonds in Deutschland? In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2002, pp. 447-452.

Barak, Aharon, Proportionality. Constitutional Rights and their Limitatios. Translated from the Hebrew by Doron Kalir. Cambridge 2013.

Barnard, Catherine and Peers, Steve (eds.), European Union Law, Oxford University Press 2014.

Barnard-Wills, David, Security, privacy and surveillance in European policy documents. In International Data Privacy Law (IDPL), Vol. 3, No. 3, 2013, pp. 170-180.

Basile, Mark, Going to the Source: Why Al Quaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing. In Studies in Conflict & Terrorism 27:3 (2004), pp. 169-185.

Baum, Gerhart, Unerledigte Verfassungsaufträge. In Datenschutz und Datensicherheit (DuD) 9 2011, pp. 595-597.

Baum, Gerhart, Wacht auf, es geht um die Menschenwürde. In Datenschutz und Datensicherheit (DuD) 9 2013, pp. 583-584.

Baum, Gerhart, Hirsch, Burkhard, Leutheusser-Schnarrenberger, Sabine, Grundrechte und Sicherheitsaufgaben des Staates – ein europäisches Thema. In Datenschutz und Datensicherheit (DuD) 6 2017, pp. 337-342.

Beccaria, Cesare, An essay on crimes and punishments. Translated by Ingraham, Edward D. (Edward Duncan), Philadelphia 1819.

Beck, Benjamin, Bitcoins als Geld im Rechtssinne. In Neue Juristische Wochenschrift (NJW) 2015, pp. 580-586.

Becker, Carlos and Seubert, Sandra, Privatheit, kommunikative Freiheit und Demokratie. In Datenschutz und Datensicherheit (DuD) 2 2016, pp. 73-78.

Beckmann, Christian, Verfassungwidrigkeit des länderübergreifenden Abrufs und der Verwendung von Daten gemäß § 88b AO. In Deutsches Steuerrecht (DStR) 2017, pp. 971-976.

Beckschäfer, Sebastian, Gesetzgeberische Reaktion auf die „Panama-Papers". In Zeitschrift für Rechtspolitik (ZRP) 2017, pp. 41-43.

Benn, Stanley I., Privacy, freedom, and respect for persons. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Bender, David, Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective. In International Data Privacy Law (IDPL), Vol. 6, No. 2, 2016, pp. 117-138.

Bentham, Jeremy, An Introduction To The Principles Of Morals And Legislation. Originally published in 1789, this edition Oxford, 1907.

Bentham, Jeremy, Panopticon; or the Inspection-House: containing the Idea of a new Principle of Construction applicable to any sort of Establishment, in which Persons of any Description are to be kept under Inspection; and in particular to Penitentiary-Houses, Prisons, Houses of Industry, Work-Houses, Poor-Houses, Lazarettos, Manufactories, Hospitals, Mad-Houses, and Schools: with a Plan of Management adapted to the Principle: In a Series of Letters, written in the Year 1787, from Crecheff in White Russia to a Friend in England. This edition Dublin 1791.

Bergemann, Nils, Verdeckte Ermittlung á la stopp: Ein unzureichender Regelungsversuch. In Datenschutz und Datensicherheit 8 2007, pp. 581-585.

Bergles, Siegfried, and Eul, Harald, Warndateien für international agierende Banken – vereinbar mit Datenschutz und Bankgeheimnis? In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2001, pp. 273-380.

Bieker, Felix and Hansen, Marit, Normen des technischen Datenschutzes nach der europäischen Datenschutzreform. In Datenschutz und Datensicherheit (DuD) 5 2017, pp. 285-289.

Bier, Christoph, Data Provenance. Technische Lösungskonzepte für das Datenschutzrecht auf Auskunft. In Datenschutz und Datensicherheit (DuD) 11 2015, pp. 741-746.

Bilsdorfer, Peter, Die Entwicklung des Steuerstraf- und Steuerordnungswidrigkeitenrechts. In Neue Juristische Wochenschrift (NJW) 2017, pp. 1525-1529.

Birnstill, Pascal and Bretthauer, Sebastian and Greiner, Simon and Krempel, Erik, Privacy-preserving surveillance: an interdisciplinary approach. In International Data Privacy Law (IDPL), Vol. 5, No. 4, 2015, pp. 298-308.

Bizer, Johann, Sieben Goldene Regeln des Datenschutzes. In Datenschutz und Datensicherheit (DuD) 5 2007, pp. 350-356. Designated as 2007a.

Bizer, Johann, Vorratsdatenspeicherung: Ein fundamentaler Verfassungsverstoß. In Datenschutz und Datensicherheit (DuD) 8 2007, pp. 586-589. Designated as 2007b.

Bloustein, Edward J., Privacy as an aspect of human dignity – An Answer to Dean Prosser. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Blume, Peter, The inherent contradictions in data protection law. In International Data Privacy Law (IDPL), Vol. 2, No. 1, 2012, pp. 26-34.

Boehm, Franziska, Datenschutz in der Europäischen Union. In Juristische Arbeitsblätter (JA) 2009, pp. 435-439.

Boehm, Franziska, Data processing and Law enforcement access to information systems at EU level. No consistent framework in spite of the envisaged data protection reform. In Datenschutz und Datensicherheit (DuD) 5 2012, pp. 339-343.

Boehm, Franziska and De Hert, Paul, Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law. In European Journal of Law and Technology, Vol. 3, No. 3, 2012.

Boehm, Franziska and Pesch, Paulina, Bitcoins: Rechtliche Herausforderungen einer virtuallen Währung – Eine erste juristische Einordnung. In MultiMedia und Recht (MMR) 2014, pp. 75-79.

Boehme-Neßler, Volker, Privacy: a matter of democracy. Why democracy needs privacy and data protection. In International Data Privacy Law (IDPL), Vol. 6 No. 3, 2016, pp. 222-229. Designated as 2016a.

Boehme-Neßler, Volker, Das Ende der Anonymität. Wie Big Data das Datenschutzrecht verändert. In Datenschutz und Datensicherheit (DuD) 7 2016, pp. 419-423. Designated as 2016b.

Böhme, Rainer and Christin, Nicolas and Edelman, Benjamin G. and Moore, Tyler, Bitcoin (July 15, 2014). Journal of Economic Perspectives, Forthcoming; Harvard Business School NOM Unit Working Paper No. 15-015. Available at SSRN: http://ssrn.com/abstract=2495572

Böhme, Rainer and Pesch, Paulina, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. In Datenschutz und Datensicherheit (DuD) 8 2017, pp. 473-481.

Bonaiuti, Gianni, Economic Issues on M-Payments and Bitcoin. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 27-51.

Borgers, Matthias J., Regulering en bestrijding van ondergronds bankieren. In: Henk van de Bunt, Dina Siegel (eds.), Ondergronds bankieren in Nederland, 2009, pp. 147-172.

Bou-Habib, Paul, Security, Profiling and Equality. In Ethical Theory and Moral Practice, Vol. 11, No. 2 (Apr., 2008), pp. 149-164.

Bou-Habib, Paul, Racial Profiling and Background Injustice. In The Journal of Ethics, Vol. 15, No. 1/2, Racial Profiling (March/June 2011), pp. 33-46.

Böszörmenyi, Janos and Schweighofer, Erich, A review of tools to comply with the Fourth EU anti-money laundering directive. In International Review of Law, Computers & Technology, 29:1 2015, pp. 63-77.

Brown, Ian, Government access to private-sector data in the United Kingdom. In International Data Privacy Law (IDPL), Vol. 2 No. 4, 2012, pp. 230-238.

Brubaker, Rogers and Cooper, Frederick, Beyond "Identity". Theory and Society 29: 1-47, 2000

Brunst, Phillip W., Staatlicher Zugang zur digitalen Identität. Erosion der Anonymität im Internet. In Datenschutz und Datensicherheit (DuD) 9 2011, pp. 618-623.

Buchmann, Erik, Wie kann man Privatheit messen? Privatheitsmaße aus der Wissenschaft. In Datenschutz und Datensicherheit (DuD) 8 2015, pp. 510-514.

Buchner, Benedikt, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. In Datenschutz und Datensicherheit (DuD) 3 2016, pp. 155-161.

Bull, Hans Peter, Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese? In Neue Juristische Wochenschrift (NJW) 2006, pp. 1617-1624.

Bülow, Karoline, Haftung der Europäischen Union nach Art. 340 Abs. 2 AEUV am Beispiel der rechtswidrigen Listung eines Terrorverdächtigen. In Europarecht (EuR) 2013, p. 609-619.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Jahresbericht der Bundesanstalt für Finanzdienstleistungsaufsicht 2016. Accessible online at https://www.bafin.de/DE/PublikationenDaten/Jahresbericht/Jahresbericht2016/jahresbericht_node.html

Bundeskriminalamt, Jahresbericht 2014, Financial Intelligence Unit (FIU) Deutschland. Accessible online at https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/FIU/Jahresberichte/fiuJahresbericht2014.html?nn=28276

Bundeskriminalamt, Jahresbericht 2016, Financial Intelligence Unit (FIU) Deutschland. Accessible online at https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/FIU/Jahresberichte/fiuJahresbericht2016.html?nn=28276

Bundesministerium der Finanzen (BMF), Der Missbrauch des Finanzsystems durch „Underground Banking" – Bestandsaufnahme und Gegenmaßnahmen. Monatsbericht 10.2004.

Bures, Oldrich, Ten Years of EU's Fight against Terrorist Financing: A Critical Assessment. In Intelligence and National Security, 30:2-3 2015, 207-233, DOI: 10.1080/02684527.2014.988443

Cannataci, Joseph A., Lex Personalitatis & Technology-driven Law. In SCRIPTed Volume 5, Issue 1, April 2008, pp 1-6.

Cannataci, Joseph A., Privacy, Technology Law and Religions across Cultures. In Journal of Information, Law & Technology (JILT), 1, May 2009, pp. 1-22.

Cannataci, Joseph A., Defying the logic, forgetting the facts: the European proposal for data protection in the police sector. In European Journal of Law and Technology, Vol. 4, Issue 2, 2013.

Carlé, Thomas, Rechtsprechung stärkt Finanzverwaltung – Reichweite der abgabenrechtlichen Auskunftspflichten. In Neue Juristische Wochenschrift (NJW) 2007, pp. 2226-2228.

Carper, Thomas R., Opening Statement, in Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf

Carr, Indira, Anonymity, the Internet and Criminal Law Issues. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 185-206.

Casagran, Cristina Blasi, Global Data Protection in the Field of Law Enforcement – An EU Perspective. Routledge 2017.

Caspar, Johannes, The CJEU Google Spain Decision. Applicability of National Data Protection Law and Consequences for the EU-Data Protection Regulation. In Datenschutz und Datensicherheit (DuD) 9 2015, pp. 589-592.

Cate, Fred H. and Cate, Beth E., The Supreme Court and information privacy. In International Data Privacy Law (IDPL), Vol. 2, No. 4, 2012, pp. 255-267.

Chen, Jiahong, How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation. In International Data Privacy Law (IDPL), Vol. 6, No. 4, 2016, pp. 310-323.

Christoffersen, Jonas, Fair Balance : Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights. International Studies in Human Rights, Volume 99, Leiden 2009.

Cicero, Marcus Tullius, On the Laws. Translated by David Fott. Ithaca, 2014.

Clarke, Roger, Data retention as mass surveillance: the need for an evaluative framework. In International Data Privacy Law (IDPL), Vol. 5, No. 2, 2015, pp. 121-132.

Cohen, Felix S. (1935), Transcendental Nonsense and the Functional Approach. Columbia Law Review, Vol. 35, No. 6 (Jun., 1935), pp. 809-849.

Collins, Richard, The unknown unknowns – risks to the banking sector from the dark side of the shadow economy. In Company Lawyer 2005, 26(3), pp. 84-87.

Constant, Benjamin, Principles of Politics Applicable to all Governments. First published in 1815, this translation by Dennis O'Keeffe, ed. Etienne Hofmann, with an Introduction by Nicholas Capaldi (Indianapolis: Liberty Fund, 2003).

Craig, Paul, Unreasonableness and Proportionality in UK Law. In: The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart 1999.

Craig, Paul and de Búrca, Gráinne, EU Law, Texts, Cases, and Materials. Oxford University Press, sixth edition 2015.

Cuéllar, Mariano-Florentino, The Tenuous Relationship between the Fight against Money Laundering and the Disruption of Criminal Finance. In The Journal of Criminal Law & Criminology, Vol. 93 Nos. 2-3, 2003, pp. 311-464.

Cunha, Mario Viola de Azevedo and Marin, Luisa and Sartor, Giovanni, Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web. In International Data Privacy Law (IDPL), Vol. 2, No. 2, 2012, pp. 50-67.

Cupa, Basil, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware). In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 419-428.

Custers, Bart and Vergouw, Bas, Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies. In Computer Law & Security Review 31 (2015), pp. 518-526.

Custers, Bart and Uršič, Helena, Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. In International Data Privacy Law (IDPL), Vol. 6, No. 1, 2016, pp. 4-15.

Danwitz, Thomas von, Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten. Die jüngere Rechtsprechung des Gerichtshofes der Europäischen Union. In Datenschutz und Datensicherheit (DuD) 9 2015, pp. 581-585.

Datta, Kavita, Risky Migrants? Low-paid migrant workers coping with financial exclusion in London. In European Urban and Regional Studies 2009 16(4), pp. 331-344.

De Andrade, Norberto Nuno Gomes and Chen-Wilson, Lisha and Argles, David and Wills, Gary and Di Zenise, Michele Schiano, Electronic Identity (2014). SpringerBriefs in Cybersecurity, DOI: 10.1007/978-1-4471-6449-4_1

De Búrca, Gráinne, The Principle of Proportionality and its Application in EC Law. In Yearbook of European Law, Volume 13, Issue 1, 1 January 1993, pp. 105-150.

De Búrca, Gráinne, Proportionality and Wednesbury Unreasonableness: The Influence of European Legal Concepts on UK Law. In European Public Law, Volume 3 (1997), Issue 4, pp. 561–586

De Búrca, Gráinne, The Road not Taken: The European Union as a Global Human Rights Actor. In The American Journal of International Law, Vol. 105, No. 4 (October 2011), pp. 649-693

De Filippi, Primavera, Bitcoin: A Regulatory Nightmare to a Libertarian Dream (May 14, 2014). In Internet Policy Review, 3(2). Available at SSRN: http://ssrn.com/abstract=2468695

De Goede, Marieke, The Politics of Preemption and the War on Terror in Europe. In European Journal of International Relations (EJIR) Vol. 14(1) 2008, pp. 161-185. Designated as 2008a.

De Goede, Marieke, Money, media and the anti-politics of terrorist finance. In European Journal of Cultural Studies, Vol. 11(3), 2008, pp. 289-310. Designated as 2008b.

De Goede, Marieke, Blacklisting and the ban: Contesting targeted sanctions in Europe. In Security Dialogue 42(6), 2011, pp. 499-515.

De Hert, Paul, The Case of Anonymity in Western Political Philosophy – Benjamin Constant's Refutation of Republican and utilitarian Arguments against Anonymity. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 47-97.

Deighton, John, Market Solutions to Privacy Problems? In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 137-146.

De Quincey, Thomas, Narrative And Miscellaneous Papers, in two Volumes. Boston, Ticknor and Fields, 1854.

DePaulo, Bella M. and Wetzel, Chris, and Sternglanz, R. Weylin, and Wlker Wilson, Molly J., Verbal and Nonverbal Dynamics of Privacy, Secrecy, and Deceit. In Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 391-410.

Diderot, Denis, Pensées philosophiques. The Hague, 1746.

Diderot, Denis, and d'Alembert, Jean le Rond, Encyclopédie, ou dictionnaire raisonné des sciences, des arts et des métiers. Published 1751-1772. University of Chicago: ARTFL Encyclopédie Project (Spring 2016 Edition), Robert Morrissey and Glenn Roe (eds.), http://encyclopedie.uchicago.edu/

Diehl, Malte, Kryptographiegesetzgebung im Wandel. Von begrenzten Schlüssellängen zur Schlüsselherausgabe. In Datenschutz und Datensicherheit (DuD) 4 2008, pp. 243-247.

Diggelmann, Oliver, and Cleis, Maria Nicole, How the Right to Privacy became a Human Right. In Human Rights Law Review, 2014, 14, p. 441-158.

Dinev, Tamara and Hart, Paul and Mullen, Michael R., Internet privacy concerns and beliefs about government surveillance – An empirical investigation. In Journal of Strategic Information Systems 17 (2008), pp. 214-233.

Dittrich, Kurt, and Trinkaus, Marc, Die gesetzlichen Regelungen der Geldwäsche und ihre Reform – eine Praxisanalyse. In Deutsches Steuerrecht (DStR) 1998, pp. 342-347.

Dix, Alexander and Petri, Thomas B., Das Fernmeldegeheimnis und die deutsche Verfassungsidentität. Zur Verfassungswidrigkeit der Vorratsdatenspeicherung. In Datenschutz und Datensicherheit (DuD) 9 2009, pp. 531-535.

Docksey, Christopher, Four fundamental rights: finding the balance. In International Data Privacy Law (IDPL), Vol. 6, No. 3, 2016, pp. 195-209.

Doi, Takeo, The Anatomy of Self – The Individual versus Society. Translated from the Japanese by Mark A. Harbison, Foreword by Edward Hall. Originally published in 1985, English translation Kodansha International 1986.

Donisthorpe, Wordsworth, Law In A Free State. Macmillan and Co., London 1895.

Dowd, Kevin, New Private Monies: A Bit-Part Player? (June 17, 2014). Institute of Economic Affairs Monographs, Hobart Paper 174. Available at SSRN: https://ssrn.com/abstract=2535299

Durner, Wolfgang, Zur Einführung: Datenschutzrecht. In Juristische Schulung, Zeitschrift für Studium und Referendariat (JuS) 2006, pp. 213-217.

Dworkin, Ronald (1977) Taking Rights Seriously. Duckworth 1977.

Dwyer, Gerald P., The Economics of Bitcoin and Similar Private Digital Currencies (July 8, 2014). Available at SSRN: http://ssrn.com/abstract=2434628 or http://dx.doi.org/10.2139/ssrn.2434628

Edwards, Lilian and Howells, Geraint, Anonymity, Consumers and the Internet: Where Everyone knows You're a Dog. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 207-247.

Eichler, Carolyn and Weichert, Thilo, EC-Kartennutzung, elektronisches Lastschriftverfahren und Datenschutz. In Datenschutz und Datensicherheit (DuD) 3 2011, pp. 201-209.

Einzinger, Kurt and Skopik, Florian and Fiedler, Roman, Keine Cyber-Sicherheit ohne Datenschutz. Datenschutzrechtliche Herausforderungen bei der Etablierung von nationalen CERTs. In Datenschutz und Datensicherheit (DuD) 11 2015, pp. 723-729.

Elias, Norbert, The Civilizing Process: State Formation and Civilization. Originally published in 1939. Translated from the German by Edmund Jephcott with some notes and revisions by the author, Oxford 1982.

Emmert, Ulrich, Europäische und nationale Regulierungen. Konsequenzen für den Datenschutz nach dem Ende von Safe Harbor. In Datenschutz und Datensicherheit (DuD) 1 2016, pp. 34-37.

Ercanbrack, Jonathan, The regulation of Islamic finance in the United Kingdom. In Ecclesiastical Law Journal 2011, 13(1), pp. 69-77.

Esayas, Samson Yoseph, The role of anonymization and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. In European Journal of Law and Technology, Vol. 6, No. 2 (2015).

European Banking Authority, EBA Opinion on 'virtual currencies'. EBA/Op/2014/08, 4 July 2014.

European Central Bank, Payments Statistics (full report) 2015, published on 26 September 2016, available online at http://sdw.ecb.europa.eu/reports.do?node=1000004051

European Central Bank, Opinion of the European Central Bank on a Proposal for a Directive of the European Parliament and of the Council 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 Directive 2009/101/EC (CON/2016/49). 13303/16, Brussels, 14 October 2016.

European Commission, Directorate-General for Employment, Social Affairs and Inclusion (European Commission), Affirming fundamental rights in the European Union – Time to act: Report of the Expert Group on Fundamental Rights. Luxembourg, February 1999.

European Commission, EU Survey on workers' remittances from the EU to third countries. Brussels, 28 April 2004, ECFIN/235/04-EN (rev 1).

European Commission (2011), Commission Staff Working Paper SEC(2011) 907, executive summary of the Impact Assessment. Available at http://ec.europa.eu/finance/finservices-retail/docs/inclusion/sec_2011_907_en.pdf

European Commission (2013), COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, SWD/2013/0164 final

European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, COM (2013) 45, Procedure 2013/0025/COD, Strasbourg, 5 February 2013.

European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism, COM/2015/0625 final, Procedure 2015/0281 (COD). Brussels, 2 December 2015

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on an Action Plan for strengthening the fight against terrorist financing, COM/2016/050 final, including Annex 1. Strasbourg, 2 February 2016.

European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 Directive 2009/101/EC, COM/2016/0450 final - 2016/0208 (COD). Strasbourg, 5 July 2016.

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Communication on further measures to enhance transparency and the fight against tax evasion and avoidance, COM/2016/0451 final. Strasbourg, 5 July 2016.

European Commission, Press release of 5 July 2016 IP/16/2380, to be found at http://europa.eu/rapid/press-release_IP-16-2380_en.htm.

European Commission, Proposal for a COUNCIL DIRECTIVE amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, COM/2016/0452 final - 2016/0209 (CNS). Strasbourg, 5 July 2016.

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM). Brussels, 29 April 2013.

European Data Protection Supervisor, Guidelines on data protection in EU financial services regulation. Brussels, 26 November 2014.

European Data Protection Supervisor, Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Fund regarding Anti-Money Laundering and Financing of Terrorism (AML-CFT) data processing. Brussels, 13 May 2015.

European Data Protection Supervisor, Opinion 6/2015: A further step towards comprehensive EU data protection – EDPS recommendations on the Directive for data protection in the police and justice sector. 28 October 2015.

European Data Protection Supervisor, Opinion 1/2017: EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC. Access to beneficial ownership information and data protection implications. 2. February 2017.

European Economic and Social Committee, Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 206/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. 13666/16, Brussels, 25 October 2016.

European Union Agency for Fundamental Rights (FRA) and Council of Europe, Handbook on European data protection law, Publications Office of the European Union, Luxembourg, April 2014

European Union Agency for Fundamental Rights (FRA), Data retention across the EU 2016. Accessible online at http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

Eymann, Torsten and Utz, Christine and Süptitz, Thomas, State-of-the-Art: Ermittlungen in der Cloud. Sicherstellung und Beschlagnahmung von Daten bei Cloud Storage-Betreibern. In Datenschutz und Datensicherheit (DuD) 5 2013, pp. 307-312.

Fan, Chun-I and Huang, Vincent Shi-Ming, Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment. In IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews, Vol. 40, No. 5, September 2010, pp. 567-579.

FATF, Combating the Abuse of Alternative Remittance Systems: International Best Practices. June 2003.

FATF, Money Laundering and Terrorist Financing Typologies 2004-2005. June 2005.

FATF, Money Laundering and Terrorist Financing in the Securities Sector. FATF Report, October 2009.

FATF, International standards on combating money laundering and the financing of terrorism and proliferation: the FATF Recommendations, February 2012.

FATF, The Role of Hawala and other similar Service Providers in Money Laundering and Terrorist Financing. FATF Report, October 2013.

FATF, Virtual Currencies – Key Definitions and Potential AML/CFT risks. FATF Report, June 2014.

FATF, Virtual Currencies – Guidance for a Risk-based Approach, June 2015.

FATF, Money Laundering through the Physical Transportation of Cash. FATF Report, October 2015.

FATF, Money or Value Transfer Services – Guidance for a Risk-based Approach, February 2016.

FATF, Consolidated FATF Standards on Information Sharing. Relevant exerpts from the FATF Recommendations and Interpretive Notes, June 2016.

Favarel-Garrigues, Gilles and Godefroy, Thierry and Lascoumes, Pierre, Reluctant Partners? Banks in the fight against money laundering and terrorism financing in France. In Security Dialogue, Special Issue on The Global Governance of Security and Finance, 42(2) 2011, pp. 179-196

Fearon, James D. (1999) What is Identity (as we now use the word)? (unpublished manuscript). https://web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/What-is-Identity-as-we-now-use-the-word-.pdf

Feiler, Lukas, The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. In European Journal of Law and Technology, Vol. 1, Issue 3, 2010.

Feldman, David, Proportionality and the Human Rights Act 1998. In: The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart 1999.

Ferret, Jérôme, "Think Little": For a Sociology of Local Regimes of Surveillance. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 324-332.

Fisahn, Andreas and Ciftci, Ridvan, Hierarchie oder Netzwerk – Zum Verhältnis nationaler zur europäischen Rechtsordnung. In Juristische Arbeitsblätter (JA) 2016, pp. 364-370.

Fisch, Markus, Das neue Transparenzregister und seine Auswirkungen auf die Praxis. In Neue Zeitschrift für Gesellschaftsrecht (NZG) 2017, pp. 408-411.

Fläming, Christian, Der Steuerstaat auf dem Weg in den Überwachungsstaat – Stellungnahme zu dem Entwurf zur Anzeigepflicht von Steuergestaltungen. In Beihefter zu Deutsches Steuerrecht (DStR) 44 2007, pp. 2-12.

Forgó, Nikolaus and Jlussi, Dennis and Klügel, Christian and Krügel, Tina, Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung. Europa tut sich schwer. In Datenschutz und Datensicherheit (DuD) 10 2008, pp. 680-682.

Fraenkel, Reinhard and Hammer, Volker, Vom Staats- zum Verfassungstrojaner. In Datenschutz und Datensicherheit (DuD) 12 2011, pp. 887-889.

Frasher, Michelle, Multinational Banking and Conflicts among US-EU AML/CFT Compliance & Privacy Law: Operational & Political Views in Context. SWIFT Institute Working Paper No. 2014-008, Published 1 July 2016.

Freiling, Felix C. and Heinson, Dennis, Probleme des Verkehrsdatenbegriffs im Rahmen der Vorratsdatenspeicherung. In Datenschutz und Datensicherheit (DuD) 9 2009, pp. 547-552.

Freund, Caroline L. and Spatafora, Nicola, Remittances: Transaction Costs, Determinants, and Informal Flows (August 2005). World Bank Policy Research Working Paper No. 3704. Available at SSRN: http://ssrn.com/abstract=803667

Fried, Charles, Privacy [A moral analysis]. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Friese, Arne and Brehm, Christian, Das neue Transparenzregister: Effektiver Kampf gegen Geldwäsche oder Bürokratie-Monstrum? In Gesellschafts- und Wirtschaftsrecht (GWR) 2017), pp. 271-274.

Froomkin, A. Michael, Anonymity in the Balance. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 5-46.

Frowd, Philippe M., SPOT the Terrorist: Border Security and the Behavioural Profiling Paradigm. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 403-415.

Fuster, Gloria González, EU Data Protection and Future Payment Services. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 181-201.

Galetta, Antonella, The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies? In European Journal of Law and Technology, Vol. 4, No. 2, 2013.

Gavison, Ruth, Privacy and the limits of law. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

General Secretariat of the Council, Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 206/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC = Negotiating Mandate. Fifth Presidency compromise text 15605/16, Brussels, 19 December 2016.

General Secretariat of the Council, Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 206/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC = Negotiating Mandate – Statements. 15615/16 ADD 1, Brussels, 19 December 2016.

Galenkamp, Marlies, Individualism versus Collectivism. The concept of collective rights (1998), Sanders Instituut, Erasmus Universiteit Rotterdam

Gärtner, Hauke and Kipker, Dennis-Kenji, Die Neuauflage der Vorratsdatenspeicherung. Lösungsansätze für zentrale Kritikpunkte am aktuellen Gesetzesentwurf. In Datenschutz und Datensicherheit (DuD) 9 2015, pp. 593-599.

Gellert, Raphaël, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. In International Data Privacy Law (IDPL), Vol. 5, No. 1, 2015, pp. 3-19.

Gerlach, Carina Sophie, Sanktionierung von Bankmitarbeitern nach dem Geldwäschegesetz-Entwurf. In Corporate Compliance Zeitschrift (CCZ) 2017, pp. 176-179.

Gerstein, Robert S., Privacy and self-incrimination. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984. Designated as 1984a.

Gerstein, Robert S., Intimacy and Privacy. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984. Designated as 1984b.

Gerven, Walter van, The Effect of Proportionality on the Actions of Member States of the European Community: National Viewpoints from Continental Europe. In: The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart 1999.

Geva, Benjamin, Mobile Payments and Bitcoin: Concluding Reflections on the Digital Upheaval in Payments. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 271-287.

Giambelluca, Gino and Masi, Paola, The Regulatory Machine: An Institutional Approach to Innovative Payments in Europe. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 3-25.

Gietl, Andreas and Tomasic, Lovro, Kompetenz der Europäischen Gemeinschaft zur Einführung der Vorratsdatenspeicherung. Anmerkung zu den Schlussanträgen von Generalanwalt Yves Bot im Verfahren C-301/06 vom 14.10.2008. In Datenschutz und Datensicherheit (DuD) 12 2008, pp. 795-800.

Gietl, Andreas, Die Zukunft der Vorratsdatenspeicherung. Anmerkung zum Urteil des BVerfG vom 2. März 2010. In Datenschutz und Datensicherheit (DuD) 6 2010, pp. 398-403.

Gilbert, David, Cryptocurrency News Round-Up: Aphroditecoin Woos Miners as Auroracoin Airdrop Nears (24 March 2014), International Business Times. Available online: http://www.ibtimes.co.uk/cryptocurrency-news-round-aphroditecoin-woos-miners-auroracoin-airdrop-nears-1441618

Glaessner, Thomas and Kellerman, Tom and McNevin, Valerie, Electronic Security: Risk Mitigation in Financial Transactions - Public Policy Issues (July 2002). World Bank Policy Research Working Paper No. 2870. Available at SSRN: http://ssrn.com/abstract=636234

Gleason, Philip, Identifying Identity: A Semantic History (March 1983). In The Journal of American History Vol. 69, No 4, pp. 910-931, 1983.

Glos, Alexander and Hildner, Alicia and Glasow, Falko, Der Regierungsentwurf zur Umsetzung der Vierten EU-Geldwäscherichtlinie – Ausweitung der geldwäscherechtlichen Pflichten außerhalb des Finanzsektors. In Corporate Compliance Zeitschrift (CCZ) 2017, pp. 83-89.

Goemans, Caroline and Dumortier, Jos, Enforcement Issues – Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-line Anonymity. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 161-183.

Goffman, Erving, Stigma. Notes on the Management of Spoiled Identity. Prentice-Hall, New Jersey, 1963.

Golden, Thomas W. and Skalak, Steven L. and Clayton, Mona M. and Pill, Jessica S., A Guide to Forensic Accounting Investigation. Second Edition, Wiley, New Jersey 2011.

Goldschmidt, Patrick and Bunk, Patrick, Big Data und die Dual-Use Problematik am Beispiel öffentlicher Daten. In Datenschutz und Datensicherheit (DuD) 7 2016, pp. 463-467.

González, Iker Barbero and Besa, Cristina Fernández, Beyond Surveillance: Ethnic Profiled Detention Practices in Everyday Life. In: C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 295-304.

Gordon, Richard and Morriss, Andrew P., Moving Money: International Financial Flows, Taxes, and Money Laundering. In 37 Hastings International and Comparative Law Review 1 (2014), pp. 1-120.

Göres, Ulrich L., Zur Rechtmäßigkeit des automatisierten Abrufs von Kontoinformationen – Ein weiterer Schritt zum gläsernen Bankkunden. In Neue Juristische Wochenschrift (NJW) 2005, pp. 253-257.

Gouvin, Eric J., Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism. In Baylor Law Review, Vol. 55, 2003, pp. 955-990.

Gouvin, Eric J., Are There Any Checks and Balances on the Government's Power to Check Our Balances? The Fate of Financial Privacy in the War on Terror (2005). In Temple Political and Civil Rights Law Review, Vol. 14, 2005, pp. 517-541.

Grafenstein, Maximilian von, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit. Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO. In Datenschutz und Datensicherheit (DuD) 12 2015, pp. 789-795.

Greenleaf, Graham, The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. In International Data Privacy Law (IDPL), Vol. 2, No. 2, 2012, pp. 68-92.

Grijpink, Jan and Prins, Corien, New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 249-269.

Grimm, Rüdiger and Bräunlich, Katharina, Vertrauen und Privatheit. Anwendungen des Referenzmodells für Vertrauen auf die Prinzipien des Datenschutzes. In Datenschutz und Datensicherheit (DuD) 5 2015, pp. 289-294.

Grudzien, Waldemar, Biometrie im Banking – Ein Plädoyer gegen Vorurteile. In Datenschutz und Datensicherheit (DuD) 1 2015, pp. 7-11.

Guggenberger, Nikolas, Das Netzwerkdurchsetzungsgesetz in der Anwendung. In Neue Juristische Wochenschrift (NJW) 2017, pp. 2577-2582

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes. In Neue Juristische Wochenschrift (NJW) 2010, pp. 1035-1041.

Haase, Adrian and Peters, Emma, Ubiquitous computing and increasing engagement of private companies in governmental surveillance. In International Data Privacy Law (IDPL), Vol. 7, No. 2, 2017, pp. 126-136.

Hadjimatheou, Katerina, The Relative Moral Risks of Untargeted and Targeted Surveillance. In Ethical Theory and Moral Practice (2014) 17, pp. 187-207

Hamacher, Rolfjosef, Der heimliche Kontenzugriff und das Grundgesetz – Finanzbehörden als Geheimdienst? In Deutsches Steuerrecht (DStR) 2006, pp. 633-638.

Hammer, Volker and Knopp, Michael, Datenschutzinstrumente Anonymisierung, Pseudonyme und Verschlüsselung. In Datenschutz und Datensicherheit (DuD) 8 2015, pp. 503-509.

Hansen, Marit, Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge? In Datenschutz und Datensicherheit (DuD) 9 2016, pp. 587-591.

Harper, David, Conspiracy or Confusion? Rumour, Contemporary Legends and Public Understanding of the Use of Personal Information. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 118-130.

Heine, Alexander, Steuerdaten im Fokus des Datenschutzes. In Datenschutz und Datensicherheit (DuD) 6 2017, pp. 368-370.

Hendrickson, Joshua R. and Hogan, Thomas L. and Luther, William J., The Political Economy of Bitcoin (July 28, 2015). Available at SSRN: https://ssrn.com/abstract=2531518 or http://dx.doi.org/10.2139/ssrn.2531518

Hensel, Dirk, Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht. Die Bildung von Persönlichkeitsprofilen und andere Probleme der Vorratsdatenspeicherung. In Datenschutz und Datensicherheit (DuD) 9 2009, pp. 527-530.

Hern, Alex, Bitcoin hype worse than 'tulip mania', says Dutch central banker. In the Guardian, December 4th, 2013. Accessible at https://www.theguardian.com/technology/2013/dec/04/bitcoin-bubble-tulip-dutch-banker

Herrmann, Klaus, and Soiné, Michael, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz. In Neue Juristische Wochenschrift (NJW) 2011, pp. 2922-2928.

Herzog, Felix; Achtelik, Robert – Geldwäschegesetz (GwG), Verlag C.H. Beck oHG, 2 Aufl. 2014

Hetzer, Wolfgang, Geldwäsche und Terrorismus. In Zeitschrift für Rechtspolitik (ZRP) 2002, pp. 407-413.

Hetzer, Wolfgang, Deutsche Umsetzung neuer europäischer Vorgaben zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung. Europäische Zeitschrift für Wirtschaftsrecht (EUZW) 2008, pp. 560-565.

Hildebrandt, Mireille, Profiling: From Data to Knowledge. The Challenges of a crucial technology. In Datenschutz und Datensicherheit 9 2006, pp. 548-552.

Hildner, Alice, Bitcoins auf dem Vormarsch: Schaffung eines regulatorischen Level Playing Fields? In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2016, pp. 485-495.

Hingst, Kai-Michael and Lösing, Carsten, Zur Erlaubnispflichtigkeit von Finanztransfergeschäften nach dem Zahlungsdiensteaufsichtsgesetz: Hohe Anforderungen an die Betreiber von Internetplattformen mit Bezahlsystemen – zugleich Anmerkung zum Urteil des LG Köln vom 29. 9. 2011 – 81 O91/11 (in diesem Heft, S. 348ff.). In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2012, pp. 334-338.

Hinneberg, Paul (ed.), Systematische Rechtwissenschaft. Die Kultur der Gegenwart – Ihre Entwicklung und ihre Ziele. Herausgegeben von Paul Hinneberg. Berlin und Leipzig 1906.

Hinneberg, Paul (ed.), Systematische Philosophie. Die Kultur der Gegenwart – Ihre Entwicklung und ihre Ziele. Herausgegeben von Paul Hinneberg. Berlin und Leipzig 1908.

Hirsch, Burkhard, Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts – Eine notwendige Entgegnung. Erwiderung zu Schäuble, ZRP 2007, 210. In Zeitschrift für Rechtspolitik (ZRP) 2008, pp. 24-25. Designated as 2008a.

Hirsch, Burkhard, Gesellschaftliche Folgen staatlicher Überwachung. In Datenschutz und Datensicherheit (DuD) 2 2008, pp. 87-91. Designate das 2008b.

Hohenhaus, Ulf, Die Terrorismusbekämpfung im Unternehmen – 9/11 und die Folgen. In Neue Zeitschrift für Arbeitsrecht (NZA) 2016, 1046-1051.

Hohmann-Dennhardt, Christine, Freiräume – Zum Schutz der Privatheit. In Neue Juristische Wochenschrift (NJW) 2006, pp. 545-549.

Holaind, René Isidore, Natural Law and Legal Practice. Lectures delivered at the Law School of Georgetown University. Benziger Brothers, New York 1899.

Holznagel, Bernd and Tabbara, Tarik, Elektronische Zahlungsmittel im Internet – Hemmnisse durch Ausfuhrkontrollen für kryptographische Produkte? In MultiMedia und Recht (MMR) 1998, pp. 387-392.

Holznagel, Bernd and Sonntag, Matthias, A Case Study: The Janus Project. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 121-135.

Hon, W. Kuan and Millard, Christopher and Walden, Ian, The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing. In International Data Privacy Law (IDPL), Vol. 1, No. 4, 2011, pp. 211-228.

Hornung, Gerrit and Schnabel, Christoph, Data protection in Germany I: The population census decision and the right to informational self-determination. In Computer Law & Security Review, Volume 25, Issue 1, 2009, pp. 84-88. Designated as 2009a.

Hornung, Gerrit and Schnabel, Christoph, Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. In Computer Law & Security Review, Volume 25, Issue 2, 2009, pp. 115-122. Designated as 2009b.

Houssein, Mohamed Djirdeh, Somalia: The Experience of Hawala Receiving Countries. In International Monetary Fund, Monetary and Financial Systems Department (eds.), Regulatory Frameworks for Hawala and Other Remittance Systems, (International Monetary Fund, Washington D.C.), pp. 87-93

Huber, Berthold, Das Bankgeheimnis der Nachrichtendienste. Zur Neuregelung der Auskunftsersuchen der Nachrichtendienste durch das Terrorismusbekämpfungsergänzungsgesetz vom 9. 1. 2007. In Neue Juristische Wochenschrift (NJW) 2007, pp. 881-883.

Hülsse, Rainer, Even clubs can't do without legitimacy: Why the anti-money laundering blacklist was suspended. In Regulation & Governance 2 2008, pp. 459-479.

Hume, David, A Treatise of Human Nature (1738–40). Available on Project Gutenberg, http://www.gutenberg.org/ebooks/4705

Hunter, Greg W., Virtual Money Illusion and the Fundamental Value of Non-Fiat Anonymous Digital Payment Methods: Coining a (Bit of) Theory to Describe the Bitcoin Phenomenon (March 15, 2014). Available at SSRN: http://ssrn.com/abstract=2483422 or http://dx.doi.org/10.2139/ssrn.2483422

International Monetary Fund (IMF), Approaches to a Regulatory Framework for Formal and Informal Remittance Systems: Experience and Lessons. Prepared by the Monetary and Financial Systems Department, by a staff team led by Chee Sung Lee and comprising Maud Bökkerlink, Joy Smallwood and Raul Hernandez-Coss. February 17, 2005.

International Monetary Fund (IMF), World Economic Outlook Database October 2016, accessible at http://www.imf.org/external/pubs/ft/weo/2016/02/weodata/index.aspx

Jacobs, Francis G., Recent Developments in the Principle of Proportionality in European Community Law. In: The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart 1999.

Jamwal, N.S., Hawala-the invisible financing system of terrorism. In Strategic Analysis 26:2 2002, pp. 181-198.

Jaspers, Andreas, Die EU-Datenschutz-Grundverordnung. Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens. In Datenschutz und Datensicherheit (DuD) 8 2012, pp. 571-575.

Jellinek, Georg, The Declaration of the Rights of Man and of Citizens: A Contribution to Modern Constitutional History. Authorized Translation from the German by Max Farrand, Revised by the Author, New York, Henry Holt and Company, 1901.

Jellinek, Georg, Allgemeine Staatslehre. Dritte Auflage unter Verwertung des handschriftlichen Nachlasses durchgesehen und ergänzt von Dr. Walter Jellinek. Berlin, Verlag von O. Häring, 1914.

Jenkins, Richard, Social Identity (2008). Third Edition, Routledge 2008

Jeong, Sarah, The Bitcoin Protocol as Law, and the Politics of a Stateless Currency (May 8, 2013). Available at SSRN: http://ssrn.com/abstract=2294124 or http://dx.doi.org/10.2139/ssrn.2294124

Johnson, Jesper Stenberg, Islamic banking and its implications for development. In Company Lawyer 2009, 30 (5), pp. 155-160.

Jong, Sang Jo, Systematic government access to private-sector data in the Republic of Korea. In International Data Privacy Law (IDPL), Vol. 4, No. 1, 2014, pp. 21-29.

Jost, Patrick M. and Sandhu, Harjit Singh, The Hawala Alternative Remittance System and its Role in Money Laundering (2000). In International Criminal Police Organization, Lyon, France

Kaetzler, Joachim, Anforderungen an die Organisation der Geldwäscheprävention bei Bankinstituten – ausgewählte Einzelfragen. In Corporate Compliance Zeitschrift (CCZ) 2008, p. 174-180.

Kahler, Thomas, Vorratsdatenspeicherung: Wer spricht Recht? BVerfG, EuGH, EGMR und die Klage gegen die Vorratsdatenspeicherung. In Datenschutz und Datensicherheit (DuD) 7 2008, pp. 449-454.

Kaiser, Carolin, The Classification of Virtual Currencies and Mobile Payments in Terms of the Old and New European Anti-Money Laundering Frameworks. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 203-230. Designated as 2016a.

Kaiser, Carolin, Bitcoin as cash in terms of the European Anti-money laundering Directive. In IANUS n. 13_bis - Special Issue 2016, pp. 23-36, available at http://www3.unisi.it/ianus/ianus_13_bis_Special_Issue_2016.html. Designated as 2016b.

Kant, Immanuel, The Philosophy of Law: An Exposition of the Fundamental Principles of Jurisprudence as the Science of Right. Translated from the German by W. Hastie, Edinburgh, 1887.

Karg, Moritz, Die Renaissance des Verbotsprinzips im Datenschutz. In Datenschutz und Datensicherheit (DuD) 2 2013, pp. 75-79.

Karg, Moritz, Anonymität, Pseudonyme und Personenbezug revisited? In Datenschutz und Datensicherheit (DuD) 8 2015, pp. 520-526.

Karper, Irene, Sorfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofi? Zur möglichen Neubewertung des Haftungsmaßstabs. In Datenschutz und Datensicherheit (DuD) 4 2006, pp. 215-219.

Kasiyanto, Safari, Security Issues of New Innovative Payments and Their Regulatory Challenges. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 145-179.

Katzenbeisser, Stefan, Technischer Schutz vor geheimdienstlicher Überwachung. Möglichkeiten und Grenzen. In Datenschutz und Datensicherheit (DuD) 2 2016, pp. 98-100.

Kemp, Richard, Legal aspects of managing Big Data. In Computer Law & Security Review 30 (2014), pp. 482-491.

Kennedy, Duncan M., The Hermeneutic of Suspicion in Contemporary American Legal Thought. In Law and Critique, 25 (2014), pp. 92-104.

Kieck, Annika and Pohl, Dirk, Zum Anwendungsbereich des europäischen Datenschutzrechts am Beispiel des Personenstands- und Meldewesens. In Datenschutz und Datensicherheit (DuD) 9 2017, pp. 567-571.

Kielmansegg Graf, Sebastian, Die Grundrechtsprüfung. In Juristische Schulung, Zeitschrift für Studium und Referendariat (JuS) 2008, pp. 23-29.

Kilkelly, Ursula, The right to respect for private and family life – A guide to the implementation of Article 8 of the European Convention on Human Rights. Human rights handbooks, No. 1, Directorate General of Human Rights, Council of Europe, first impression, November 2001, reprinted with corrections, August 2003.

Knopp, Michael, Pseudonym – Grauzone zwischen Anonymisierung und Personenbezug. In Datenschutz und Datensicherheit (DuD) 8 2015, pp. 527-530.

Kokott, Juliane and Sobotta, Christoph, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. In International Data Privacy Law (IDPL), Vol. 3, No. 4, 2013, pp. 222-228.

Köllner, Rolf E. and Mück, Jörg, Reform der strafrechtlichen Vermögensabschöpfung. In Neue Zeitschrift für Insolvenz- und Sanierungsrecht (NZI) 2017, pp. 593-599.

Koops, Bert-Jaap, The trouble with European data protection law. In International Data Privacy Law (IDPL), Vol. 4, No. 4, 2014, pp. 250-261.

Köpsell, Stefan and Pfitzmann, Andreas, Wie viel Anonymität verträgt unsere Gesellschaft? In Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Eds.): Security, E-Learning, E-Services; 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf, GI-Edition Lecture Notes in Informatics (LNI) P-44, Bonn 2003, pp. 13-26.

Korff, Douwe, The rule of law on the Internet and in the wider digital world. Issue paper published by the Council of Europe Commissioner for Human Rights, December 2014.

Koshan, Mansoor, Vorratsdatenspeicherung – verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung. Zur Notwendigkeit einer „informationsverfassungsrechtlichen" Grundlegung. In Datenschutz und Datensicherheit (DuD) 3 2016, pp. 167-171.

Krais, Jürgen, Die Pläne zur Errichtung eines zentralen Transparenzregisters. In Corporate Compliance Zeitschrift (CCZ) 2017, pp. 98-107.

Krings, Günther, Terrorismusbekämpfung im Spannungsfeld zwischen Sicherheit und Freiheit. In Zeitschrift für Rechtspolitik (ZRP) 2015, pp. 167-170.

Kubát, Max, Virtual currency bitcoin in the scope of money definition and store of value. In Procedia Economics and Finance 30 (2015), pp. 409-416.

Kugelmann, Dieter, Datenschutz bei Polizei und Justiz. Der Richtlinienvorschlag der Kommission. In Datenschutz und Datensicherheit (DuD) 8 2012, pp. 581-583.

Kühling, Jürgen and Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? In Europäische Zeitschrift für Wirtschaftsrecht (EUZW) 2016, pp. 448-454

Kulesza, Joanna, Transboundary data protection and international business compliance. In International Data Privacy Law (IDPL), Vol. 4, No. 4, 2014, pp. 298-306.

Kunnert, Gerhard, EuGH zur Vorratsdatenspeicherung: Außer Spesen nichts gewesen? Analyse des Urteils v. 8.5.2014 (C-293/12 u. C-594/12). In Datenschutz und Datensicherheit (DuD) 11 2014, pp. 774-784.

Kütük, Merih Erdem and Sorge, Christoph, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie" zur „Bitcoinmanie". In MultiMedia und Recht (MMR) 2014, pp. 643-646.

Kutzner, Lars, "Kontenabfragen" im Rahmen des Rechtshilfeverkehrs in der Europäischen Union. In Deutsches Steuerrecht (DStR) 2006, pp. 639-644.

Lambert, Larry, Asian Underground Banking Scheme. A Field Note. In Journal of Contemporary Criminal Justice, Vol. 18 No. 4, November 2002, pp. 358-369.

Lascaux, Alexander (2015) Crowding Out Trust in the Informal Monetary Relationships: The Curious Case of the Hawala System, Forum for Social Economics, 44:1, 87-107

Lauritsen, Peter and Bøge, Ask Risom, Building an Oligopticon – A Study of Video Surveillance in Danish Police Work. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 138-144.

Lavalle, Roberto, The International Convention for the Suppression of the Financing of Terrorism. In Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV) 2000, pp. 491-510.

Leith, Philip, The socio-legal context of privacy. In International Journal of Law in Context, Volume 2, Issue 2, June 2006 , pp. 105-136.

Lennon, Genevieve and Walker, Clive, Hot money in a cold climate. In UK Public Law 2009, Jan, 37-42.

Leonard, Peter, Customer data analytics: privacy settings for 'Big Data' business. In International Data Privacy Law (IDPL), Vol. 4, No. 1, 2014, pp. 53-68.

Leslie, Daniel Adeoyé, Legal Principles for Combatting Cyberlaundering. Law Governance and Technology Series Volume 19, 2014.

Leutheusser-Schnarrenberger, Sabine, Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa. In Datenschutz und Datensicherheit (DuD) 9 2014, pp. 589-592.

Leutheusser-Schnarrenberger, Sabine, Vom Vergessen und Erinnern. Ein Jahr nach der Entscheidung des Gerichtshofs der Europäischen Union (EuGH). In Datenschutz und Datensicherheit (DuD) 9 2015, pp. 586-588.

Leutheusser-Schnarrenberger, Sabine, Der EuGH stärkt den Zusammenhalt in der Europäischen Union. In Datenschutz und Datensicherheit (DuD) 6 2016, pp. 354-356.

Lewinski, Kai von, Europäisierung des Datenschutzrechts. Umsetzungsspielraum des deutschen Gesetzgebers und Entscheidungskompetenz des BVerfG. In Datenschutz und Datensicherheit (DuD) 8 2012, pp. 564-570.

Linke, Tobias, Die Menschenwürde im Überblick: Konstitutionsprinzip, Grundrecht, Schutzpflicht. In Juristische Schulung, Zeitschrift für Studium und Referendariat (JuS) 2016, pp. 888-893.

Lioy, Diodato, The Philosophy of Right, with Special Reference to the Principles and Development of Law. Translated from the Italian by W. Hastie. Kegan Paul, Trench, Trübner & Co., London, 1891.

Liszt, Franz von, Das Völkerrecht: Systematisch Dargestellt. Berlin, 1898.

Lochen, Sebastian, Risikoanalyse. In Corporate Compliance Zeitschrift (CCZ), pp. 92-93.

Lowery, Edward, Prepared Testimony Before the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013. In: Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf

Luther, William, Regulating Bitcoin: On What Grounds? In Hester Peirce and Benjamin Klutsey (eds.), Reframing Financial Regulation. Enhancing Stability and Protecting Consumers. Mercatus Center, George Mason University 2016.

Lynskey, Orla, Deconstructing Data Protection: The 'added-value' of a Right to Data Protection in the EU Legal Order. In International and Comparative Law Quarterly Vol. 63, July 2014, pp. 569-597.

Mack, Alexandra, Aktuelles zum Kontenabruf und neue Chancen der Streitführung angesichts wachsender Verfassungsprobleme im Steuerrecht – Zugleich Anmerkungen zu den Urteilen des BFH vom 29. 11. 2005 und des FG Köln vom 22. 9. 2005. In Deutsches Steuerrecht (DStR) 2006, pp. 394-399.

Macnish, Kevin, Whose Business Is It? Authority and Surveillance. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 173-182.

Magrani, Bruno, Systematic Government access to private-sector data in Brazil. In International Data Privacy Law (IDPL), Vol. 4, No. 1, 2014, pp. 30-38.

Maidorn, Vanessa, Der automatisierte Kontenabruf – Rechtsschutz gegen einen „Realakt". In Neue Juristische Wochenschrift (NJW) 2006, pp. 3752-3757.

Malgieri, Gianclaudio, Trade Secrets v Personal Data: a possible solution for balancing rights. In International Data Privacy Law (IDPL), Vol. 6, No. 2, 2016, pp. 102-116.

Manger-Nestler, Cornelia and Noack, Gregor, Europäische Grundfreiheiten und Grundrechte. In Juristische Schulung, Zeitschrift für Studium und Referendariat (JuS) 2013, pp. 503-507.

Maras, Marie-Helen, The social consequences of a mass surveillance measure: What happens when we become the 'others'? In International Journal of Law, Crime and Justice 40 (2012), pp. 65-81.

Marnau, Ninja, Anonymisierung, Pseudonymisierung und Transparenz für Big Data. Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung. In Datenschutz und Datensicherheit (DuD) 7 2016, pp. 428-433.

Martin, Marina, Hundi/Hawala: The Problem of Definition. In Modern Asian Studies, Vol. 43, No. 4 (Jul., 2009), pp. 909-937.

Martin, Marina (2015) Project codification: legal legacies of the British Raj on the Indian mercantile credit institution hundi. In Contemporary South Asia, 23:1, 67-84.

Martini, Mario, Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, Juristische Arbeitsblätter (JA) 2009, pp. 839-845.

Marx, Gary T., A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. In Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 369-390.

Maxwell, Winston, Systematic government access to private-sector data in France. In International Data Privacy Law (IDPL), Vol. 4, No. 1, 2014, pp. 4-11.

McBride, Jeremy, Proportionality and the European Convention on Human Rights. In: The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart 1999.

Mead, George H., Mind, Self, and Society – From the Standpoint of a Social Behaviorist. Chicago 1934. This edition edited and with an Introduction by Charles W. Morris, Chicago 1962.

Meiklejohn, Sarah and Pomarole, Marjori and Jordan, Grant and Levchenko, Kirill and McCoy, Damon and Voelker, Geoffrey M. and Savage, Stefan, A Fistful of Bitcoins: Characterizing Payments among Men with No Names. In Communications of the ACM, April 2016: Vol. 59 No. 4, Pages 86-93.

Meints, Martin and Hansen, Marit, Identitätsdokumente. eIDs und maschinenlesbare Ausweise. In Datenschutz und Datensicherheit 9 2006, pp. 560-564

Meister, Andre, Secret documents reveal: German foreign spy agency BND attacks the anonymity network Tor and advises not to use it. In Netzpolitik.org, 15.09.2017. To be found at https://netzpolitik.org/2017/secret-documents-reveal-german-foreign-spy-agency-bnd-attacks-the-anonymity-network-tor-and-advises-not-to-use-it/

Mehrbrey, Kim Lars and Schreibauer, Marcus, Haftungsverhältnisse bei Cyber-Angriffen – Ansprüche und Haftungsrisiken von Unternehmen und Organen. In MultiMedia und Recht (MMR) 2016, pp. 75-82.

Mezzana, Daniele and Krlic, Marija, The current context of surveillance: An overview of some emerging phenomena and policies. In European Journal of Law and Technology, Vol. 4, No. 2, 2013.

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht. In Datenschutz und Datensicherheit (DuD) 6 2017, pp. 349-353.

Milaj, Jonida, and Mifsud Bonnici, Jeanne Pia, Unwitting subjects of surveillance and the presumption of innocence. In Computer Law and Security Review 20 (2014), 419-428.

Milaj, Jonida and Kaiser, Carolin, Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'. In International Data Privacy Law (IDPL), Volume 7, Issue 2, 1 May 2017, Pages 115–125.

Milaj-Weishaar, Jonida, Surveillance with non-purpose built technology. Challenges for the protection of the right to privacy in the European Union. Groningen 2017.

Mill, James, Elements of Political Economy. Printed for Baldwin, Craddock, and Joy, London 1821.

Mitsilegas, Valsamis and Gilmore, Bill, The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards. In International Comparative Law Quarterly (ICLQ) 2007, p. 118-140

Moerel, Lokke, Back to basics: when does EU data protection law apply? In International Data Privacy Law (IDPL), Vol. 1, No. 2, 2011, pp. 92-110.

Moerel, Lokke, GDPR conundrums: Processing special categories of data. September 12, 2016, available at https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/

Möllers, Thomas M.J. and Redcay, Katharina, Das Bundesverfassungsgericht als europäischer Gesetzgeber oder als Motor der Union? In Europarecht (EuR) 2013, pp. 409-432.

Monteleone, Shara, Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity? In European Journal of Law and Technology, Vol. 3, No. 3, 2012.

Möser, Malte and Böhme, Rainer and Breuker, Dominic, An inquiry into money laundering tools in the Bitcoin ecosystem. Published in IEEE eCrime Researchers Summit (eCRS), 2013, San Francisco, CA, USA.

Müller, Christian, und Starre, Mario, Verbot der Informationsweitergabe über Verdachtsanzeigen für Institute und Unternehmen aus EU-Mitgliedstaaten und Drittstaaten – Ein Hindernis für die effektive Geldwäschebekämpfung?, in Corporate Compliance Zeitschrift (CCZ) 2014, 23-29.

Murck, Patrick, Testimony of Patrick Murck, General Counsel, the Bitcoin Foundation, to the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013. In: Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf

Murphy, Maria Helen, Emerging Privacy Questions and New Surveillance Methods: GPS Tracking Under the European Convention on Human Rights and the Constitution of the United States of America. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 453-462.

Murphy, Robert F., Social distance and the veil. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Nabeth, Thierry, Identity of Identity. Building a Shared Understanding of the Concept of Identity in the FIDIS Network of Excellence. In Datenschutz und Datensicherheit 9 2006, pp. 538-542.

Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System [2008]. Available online at https://bitcoin.org/bitcoin.pdf

NCA, UK National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2015. Available online at http://www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015/file

Nelson, Leonard, Die Rechtswissenschaft ohne Recht. Kritische Betrachtungen über die Grundlagen des Staats- und Völkerrechts, insbesondere über die Lehre von der Souveränität. Leipzig, Verlag von Veit & Comp., 1917.

Nelson, Leonard, System der philosophischen Rechtslehre. Verlag Der Neue Geist, Leipzig 1920.

Nicoll, Chris, Concealing and Revealing Identity on the Internet. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 99-119.

Nicoll, Chris and Prins, Corien, Anonymity: Challenges for Politics and Law. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 249-269.

Novotny, Alexander and Spiekermann, Sarah, Personenbezogene Daten privat-wirtschaftlich nachhaltig nutzen. In Datenschutz und Datensicherheit (DuD) 7 2015, pp. 460-464.

Oerlemans, J.J. and Custers, B.H.M. and Pool, R.L.D. and Cornelisse, R., Cybercrime en Witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware. Onderzoek en Beleid, WODC Boom 2016.

Oostveen, Manon, Identifiability and the applicability of data protection to big data. In International Data Privacy Law (IDPL), Vol. 6, No. 4, 2016, pp. 299-309.

The P2P Foundation, Bitcoin (no date). Available online: http://p2pfoundation.net/Bitcoin

Padova, Yann, The Safe Harbor is invalid: what tools remain for data transfers and what comes next? In International Data Privacy Law (IDPL), Vol. 6, No. 2, 2016, 139-161.

Passas, Nikos, Hawala and Other Informal Value Transfer Systems: How to Regulate Them? In Risk Management, Vol. 5, NO. 2, Special Issue: Regulation, Risk and Corporate Crime in a 'Globalised' Era, 2003, pp. 49-59.

Passas, Nikos, Demystifying Hawala: A Look into its Social Organization and Mechanics. In Journal of Scandinavian Studies in Criminology and Crime Prevention Vol. 7 2006, pp. 46-62.

Pell, Stephanie K., Systematic government access to private-sector data in the United States. In International Data Privacy Law (IDPL), Vol. 2, No. 4, 2012, pp. 245-254.

Pesch, Paulina and Böhme, Rainer, Datenschutz trotz öffentlicher Blockchain? Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten. In Datenschutz und Datensicherheit (DuD) 2 2017, pp. 93-98.

Petri, Thomas B., Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung". In Datenschutz und Datensicherheit (DuD) 7 2008, pp. 443-445. Designated as 2008a.

Petri, Thomas, Unzulässige Vorratssammlungen nach dem Volkszählungsurteil? Die Speicherung von TK-Verkehrsdaten und Flugpassagierdaten. In Datenschutz und Datensicherheit (DuD) 11 2008, pp. 729-732. Designated as 2008b.

Petri, Thomas, Wertewandel im Datenschutz und die Grundrechte. In Datenschutz und Datensicherheit (DuD) 1 2010, pp. 25-29.

Petri, Thomas, Sicherheit und Selbstbestimmung – deutsche und europäische Diskurse zum Datenschutz. In Datenschutz und Datensicherheit (DuD) 8 2010, pp. 539-543.

Petri, Thomas, Die Safe-Harbor Entscheidung. Erste Anmerkungen. In Datenschutz und Datensicherheit (DuD) 12 2015, pp. 801-805.

Pfitzmann, Andreas and Köpsell, Stefan, Risiken der Vorratsdatenspeicherung. Grenzen der Nutzungsüberwachung. In Datenschutz und Datensicherheit (DuD) 9 2009, pp. 542-546.

Pieke, Frank N. and Van Hear, Nicholas and Lindley, Anna, Beyond Control? The mechanics and dynamics of 'informal' remittances between Europe and Africa. In Global Networks Vol 7 Issue 3, 2007, pp. 348-366.

Pimenidis, Lexi and Kosta, Eleni, The impact of the retention of traffic and location data on the internet user. A critical discussion. In Datenschutz und Datensicherheit (DuD) 2 2008, pp. 92-95.

Polčák, Radim, Getting European data protection off the ground. In International Data Privacy Law (IDPL), Vol. 4, No. 4, 2014, pp. 282-289.

Pocs, Matthias, Gestaltung von Fahndungsdateien. Verfassungsverträglichkeit biometrischer Systeme. In Datenschutz und Datensicherheit (DuD) 3 2011, pp. 163-168.

Pordesch, Ulrich and Steidle, Roland, Entfernen des Personenbezugs mittels Verschlüsselung durch Cloudnutzer. In Datenschutz und Datensicherheit (DuD) 8 2015, pp. 536-541.

Poscher, Ralf, Menschenwürde und Kernbereichsschutz. Von den Gefahren einer Verräumlichung des Grundrechtsdenkens. In Juristen Zeitung (JZ) 2009, pp. 269-320.

Posner, Richard A., An economic theory of privacy. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Pound, Roscoe, An Introduction to the Philosophy of Law. New Haven, Yale 1922.

Prantl, Heribert, Weltweiter Datenschutz und zukünftiger Schutz der Grundrechte. In Datenschutz und Datensicherheit (DuD) 6 2016, pp. 347-353.

Preibusch, Sören, Guide to measuring privacy concern: Review of survey and observational instruments. In International Journal of Human-Computer Studies, Volume 71, Issue 12, December 2013, Pages 1133-1143.

Privacy International, Mass Surveillance (no date). Available online: https://www.privacyinternational.org/node/52

Prosser, William L., Privacy [A legal analysis]. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Puschke, Jens and Singelnstein, Tobias, Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen. In Neue Juristische Wochenschrift (NJW) 2005, pp. 3534-3538.

Raab, Charles D., Privacy as a Security Value. In: Dag Wiese Schartum, Lee A. Bygrave and Anne Gunn Berge Bekken (eds.), Jon Bing, en hyllest. Oslo 2014, pp. 39-58.

Raabe, Oliver and Wagner, Manuela, Verantwortlicher Einsatz von Big Data. Ein Zwischenfazit zur Entwicklung von Leitplanken für die digitale Gesellschaft. In Datenschutz und Datensicherheit (DuD) 7 2016, pp. 434-439.

Rachels, James, Why privacy is important. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Raman, Mythili, Statement of Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, Before the Committee on Homeland Security and Governmental Affairs, United States Senate, November 18, 2013. In: Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf

Raphaeli, Nimrod, Financing of Terrorism: Sources, Methods, and Channels. In Terrorism and Political Violence, 15:4, 2003, pp. 59-82.

Rawls, John, Justice as Fairness. A Restatement. Harvard 2001.

Razavi, Maryam, Hawala: An underground haven for terrorists or social phenomenon? (2005). In Crime, Law & Social Change (2005) 44: 277-299, DOI: 10.1007/s10611-006-9019-3.

Razavi, Maryam and Haggerty, Kevin D., Hawala under Scrutiny: Documentation, Surveillance and Trust. In International Political Sociology 2009, Vol 3, pp. 139-155.

Reddick, Christopher G. and Chatfield, Akemi Takeoka and Jaramillo, Patricia A., Public opinion on National Security Agency surveillance programs: A multi-method approach. In Government Information Quarterly 32 (2015), pp. 129-141.

Redin, Dulce and Calderon, Reyes and Ferrero, Ignacio, Cultural Financial Traditions and Universal Ethics: The Case of Hawala (October 1, 2012). In Journal of Business Ethics, DOI: 10.1007/s10551-013-1874-0. Available at SSRN: http://ssrn.com/abstract=2486079 or http://dx.doi.org/10.2139/ssrn.2486079

Reding, Viviane, The European data protection framework for the twenty-first century. In International Data Privacy Law (IDPL), Vol. 2, No. 3, 2012, pp. 119-129.

Rees, Christopher, and Brimsted, Kate, and Smith, Herbert, Charybdis or Scylla? – Navigating a course between money laundering law and data protection. In Computer Law & Security Report Vol. 19 no. 1 2003, ISSN 0267 3649/03.

Reichling, Tilman, Massive Ausweitung der Kontenabfrage. Bundesrat forciert Zugriffsmöglichkeit auf Bankkunden-Daten für Gerichtsvollzieher und Vollstreckungsbehörden. In Datenschutz und Datensicherheit (DuD) 10 2008, pp. 670-672.

Reid, Fergal and Harrigan, Martin, An Analysis of Anonymity in the Bitcoin System (May 7, 2012). In Security and Privacy in Social Networks 2012, pp. 197–223.

Reiman, Jeffrey H., Privacy, intimacy, and personhood. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Reimer, Richard and Wilhelm, Alexander, Aktuelle Entwicklungen des Finanztransfergeschäfts. In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2008), pp. 234-241.

Resta, Giorgio, Systematic government access to private-sector data in Italy. In International Data Privacy Law (IDPL), Vol. 4, No. 1, 2014, pp. 12-20.

Richter, Philipp, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. In Datenschutz und Datensicherheit (DuD) 11 2015, pp. 735-740.

Richter, Philipp, Instrumente zwischen rechtlicher Steuerung und technischer Entwicklung. In Datenschutz und Datensicherheit (DuD) 2 2016, pp. 89-93. Designated as 2016a.

Richter, Philipp, Big Data, Statistik und die Datenschutz-Grundverordnung. In Datenschutz und Datensicherheit (DuD) 9 2016, pp. 581-586. Designated as 2016b.

Rittgen, Helmut, Bargeld – ein Zahlungsmittel von gestern? Speech delivered at the Bargeldsymposium der Deutschen Bundesbank, 10. Oktober 2012 in Frankfurt am Main.

Roberge, Ian, Misguided Policies in the War on Terror? The Case for Disentangling Terrorist Financing From Money Laundering. In Politics, Political Studies Association 2007, Vol 27(3), pp. 196-203.

Rodriguez, Katitza, Freedom of Expression, Privacy and Anonymity on the Internet, Comments submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression, January 2011, to be found at https://www.eff.org/de/Frank-La-Rue-United-Nations-Rapporteur

Romanian Chamber of Deputies, Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 206/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC [doc. 10678/16 – COM(2016) 450 final] – Opinion on the application of the Principles of Subsidiarity and Proportionality, 13576/16, Brussels, 21 October 2016.

Ronellenfitsch, Michael, Datenschutzrechtliche Schranken bei der Terrorismusbekämpfung. In Datenschutz und Datensicherheit (DuD) 8 2007, pp. 561-570.

Ronellenfitsch, Michael, Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV. In Datenschutz und Datensicherheit (DuD) 8 2009, pp. 451-461.

Roosendaal, Arnold, Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts. Oisterwijk, 2013.

Roßnagel, Alexander and Bedner, Mark and Knopp, Michael, Rechtliche Anforderungen an die Aufbewahrung von Vorratsdaten. In Datenschutz und Datensicherheit (DuD) 9 2009, pp. 536-541.

Roßnagel, Alexander, Das Bundesverfassungsgericht und die Vorratsdatenspeicherung in Europa. In Datenschutz und Datensicherheit (DuD) 8 2010, pp. 544-548.

Roßnagel, Alexander and Nebel, Maxi, (Verlorene) Selbstbestimmung im Datenmeer. Privatheit im Zeitalter von Big Data. In Datenschutz und Datensicherheit (DuD) 7 2015, pp. 455-459.

Roßnagel, Alexander, Wie zukunftsfähig ist die Datenschutz-Grundverordnung? Welche Antworten bietet sie für die neuen Herausforderungen des Datenschutzrechts? In Datenschutz und Datensicherheit (DuD) 9 2016, pp. 561-565.

Rossum, Henk van and Gardeniers, Huib, and Borking, John and Meijers, Joost and Verhaar, Paul, and Overbeek, Paul, Privacy-Enhancing Technologies: The path to anonymity, Volume II. Achtergrondstudies en Verkenningen 5b, Registratiekamer, August 1995.

Rost, Martin, Zur Soziologie des Datenschutzes. In Datenschutz und Datensicherheit (DuD) 2 2013, pp. 85-91.

Rubinstein, Ira S., Big Data: The End of Privacy or a New Beginning? In International Data Privacy Law (IDPL), Vol. 3, No. 2, 2013, pp. 74-87.

Rückert, Christian, Virtual Currencies and Fundamental Rights (August 9, 2016). Working Paper. Available at SSRN: https://ssrn.com/abstract=2820634 or http://dx.doi.org/10.2139/ssrn.2820634

Ryder, Nicholas – A false sense of security? An analysis of the legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom. Journal of Business Law (JBL) 2007, 820-850

Salom, Javier Aparicio, 'A third party to whom data are disclosed': A third group among those processing data. In International Data Privacy Law (IDPL), Vol. 4, No. 3, 2014, pp. 177-188.

Sandleben, Hans-Martin, and Wittmann, Markus, Regelungen gegen Geldwäsche im Nicht-Finanzsektor. In Zeitschrift für Bilanzierung, Rechnungswesen und Controlling (BC) 2010, pp. 464-468.

Santos, Filipe, The Dissemination and Popularisation of Surveillance Technologies: Five Case Studies of Criminal Cases. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 443-452.

Sarunski, Maik, Big Data – Ende der Anonymität? Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern. In Datenschutz und Datensicherheit (DuD) 7 2016, pp. 424-427.

Schaar, Peter, Modernisierung des Datenschutzes: Ethik der Informationsgesellschaft. In Datenschutz und Datensicherheit (DuD) 4 2007, pp. 259-263.

Schaar, Peter, Kurzgutachten zur überarbeiteten EU-Geldwäscherichtlinie. Berlin, 5. September 2016. To be found at https://www.prepaidverband.de/kurzgutachten-zur-ueberarbeiteten-eu-geldwaescherichtlinie/

Schafer, Burkhard, Surveillance for the Masses: the political and legal landscape of the UK Investigatory Powers Bill. In Datenschutz und Datensicherheit (DuD) 9 2016, pp. 592-597.

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. Neue Juristische Wochenschrift (NJW) 2016, 1841-1847.

Schaub, Peter, Das neue Transparenzregister naht – Überblick über die Regelungen und praktische Auswirkungen für Personenvereinigungen. In Deutsches Steuerrecht (DStR) 2017, pp. 1438-1444.

Schertz, Christian, Der Schutz des Individuums in der modernen Mediengesellschaft. In Neue Juristische Wochenschrift (NJW) 2013, pp. 721-728.

Schild, Hans-Herrmann and Tinnefeld, Marie-Theres, Datenschutz in der Union – Gelungene oder missglückte Gesetzentwürfe? In Datenschutz und Datensicherheit (DuD) 5 2012, pp. 312-317.

Schmale, Wolfgang and Tinnefeld, Marie-Theres, Identität durch Grundrechte. In Datenschutz und Datensicherheit (DuD) 8 2010, pp. 523-528.

Schmale, Wolfgang and Tinnefeld, Marie-Theres, Europa durch Menschenrechte. In Datenschutz und Datensicherheit (DuD) 6 2017, pp. 343-347

Schmidt, Carsten and Ruckes, Andreas, OECD Common Reporting Standard – Hintergrund, Eckpunkte und Praxisaspekte. In Internationales Steuerrecht (IStR) 2014, pp. 652-660.

Schmidt, Carsten and Ruckes, Andreas, Das Steuerumgehungsbekämpfungsgesetz – Hintergrund, Inhalte und Praxisaspekte. In Internationales Steuerrecht (IStR) 2017, pp. 473-479.

Schoeman, Ferdinand, Privacy: philosophical dimensions of the literature. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984. Designated as 1984a.

Schoeman, Ferdinand, Privacy and intimate information. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984. Designated as 1984b.

Scholz-Fröhling, Sabine, FinTechs und die bankenaufsichtsrechtlichen Lizenzpflichten. In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2017, pp. 133-139.

Schramm, Matthias and Taube, Markus (2002) The Institutional Foundations of al Qaida's Global Financial System. To be found at www.diw.de/sixcms/detail.php/39098

Schramm, Matthias and Taube, Markus, Evolution and institutional foundation of the hawala financial system. In International Review of Financial Analysis Vol. 12, 2003, pp. 405-420.

Schrey, Joachim and Thalhofer, Thomas, Rechtliche Aspekte der Blockchain. In Neue Juristische Wochenschrift (NJW) 2017, pp. 1431-1436.

Schröder, Martin and Morgner, Frank, eID mit abgeleiteten Identitäten. In Datenschutz und Datensicherheit (DuD) 8 2013, pp. 530-534.

Schröder, Ulrich Jan, Der Schutzbereich der Grundrechte. In Juristische Arbeitsblätter (JA) 2016, pp. 641-648.

Schwartz, Barry, The Social Psychology of Privacy. In American Journal of Sociology, Vol. 73, No. 6 (May, 1968), pp. 741-752.

Schwartz, Paul M., Systematic government access to private-sector data in Germany. In International Data Privacy Law (IDPL), Vol. 2, No. 4, 2012, pp. 289-301.

Schweizer, Rainer J., Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz. In Datenschutz und Datensicherheit (DuD) 8 2009, pp. 462-468.

Schwichtenberg, Simon, Die "kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz. In Datenschutz und Datensicherheit (DuD) 9 2016, pp. 605-609.

Seubert, Sandra, Der gesellschaftliche Wert des Privaten. In Datenschutz und Datensicherheit (DuD) 2 2012, pp. 100-102.

Shakespeare, William, The History of Troilus and Cressida. Originally published in 1602, this edition from the Complete Works of William Shakespeare, World Library Inc. 1993. Available at Project Gutenberg http://www.gutenberg.org/ebooks/1790

Sharma, Divya, Historical Traces of Hundi, Sociocultural Understanding, and Criminal Abuses of Hawala. In International Criminal Justice Review Volume 16 Number 2, September 2006, pp. 99-121.

Shasky Calvery, Jennifer, Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network, United States Department of the Treasury, Before the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013. In: Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies (2013) – U.S. Senate Committee on Homeland Security and Governmental Affairs, 113th Congress, First Session, accessible at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf.

Shields, Peter, The 'information revolution', financial globalisation, state power and money-laundering. In The Journal of International Communication, 11:1 2005, pp. 15-39.

Silvestri, Vico, Wie sich die Schweiz gegen Geldwäscherei schützt und was die Schweiz im Speziellen gegen die Finanzierung des Terrorismus macht. In Foertsch, Volker and Lange, Klaus, Islamischer Terrorismus – Bestandsaufnahme und Bekämpfungsmöglichkeiten. Hans Seidel Stiftung, München 2005, pp. 164-171.

Simitis, Spiros, BGH, 19. 9. 1985 – III ZR 213/83. Zur Zulässigkeit der Übermittlung von Kundendaten an die „Schufa", mit Anmerkung Simitis. In JuristenZeitung (JZ), 41 Jahrg., Nr. 4 (21 Februar 1986), pp. 185-191.

Simitis, Spiros, Datenschutz – Rückschritt oder Neubeginn? In Neue Juristische Wochenschrift (NJW) 1998, pp. 2473-2479.

Simitis, Spiros, Revisiting Sensitive Data. Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24-26 November 1999).

Simmchen, Christoph, Blockchain (R)Evolution. Verwendungsmöglichkeiten und Risiken. In MultiMedia und Recht (MMR) 2017, pp. 162-165.

Simmel, Georg, The Sociology of Secrecy and of Secret Societies. Translated by Albion W. Small. In American Journal of Sociology, Volume 11, Issue 4 (Jan., 1906), pp. 441-498.

Singelnstein, Tobias and Derin, Benjamin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. Was aus der StPO-Reform geworden ist. In Neue Juristische Wochenschrift (NJW) 2017, pp. 2646-2652.

Skouris, Vassilios, Leilinien der Rechtsprechung des EuGH zum Datenschutz. In Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, pp. 1359-1364.

Söllner, Sebastian, Bargeld im Sicherheitsrecht. In Neue Juristische Wochenschrift (NJW) 2009, pp. 3339-3343.

Solove, Daniel J., Conceptualizing Privacy. In California Law Review, Vol. 90, 2002, pp. 1087-1155.

Solove, Daniel J., "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. In San Diego Law Review, Vol. 44, pp. 745-772, 2007; GWU Law School Public Law Research Paper No. 289.

Sophocles, Antigone. In: Plays of Sophocles, with an English translation by F. Storr, London 1962.

Sorel, Jean-Marc, Some questions about the definition of terrorism and the fight against its financing. In European Journal of International Law 2003, 14(2), 365-378.

Sorge, Christoph, Datenschutz in P2P-basierten Systemen. Peer-to-Peer-Netze jenseits des Filesharing. In Datenschutz und Datensicherheit (DuD) 2 2007, pp. 102-106.

Sorge, Christoph and Krohn-Grimberghe, Artus, Bitcoin: Eine erste Einordnung. In Datenschutz und Datensicherheit (DuD) 7 2012, pp. 479-484.

Sotiriadis, Georgios, and Heimerdinger, Dominik, Die Umsetzung der 3. EG-Geldwäscherichtlinie und ihre Bedeutung für die Finanzwirtschaft. In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2009, pp. 234-241.

Soudijn, Melvin, Using strangers for money: a discussion on money-launderers in organized crime (2014). In Trends in Organized Crime (2014) 17: 199-217. DOI: 10.1007/s12117-014-9217-9

Soudijn, Melvin, Hawala and Money Laundering: Potential Use of Red Flags for Persons Offering Hawala Services. In The European Journal on Criminal Policy and Research (2015) 21, pp. 257-274.

Spindler, Gerald, Persönlichkeitsrecht und Datenschutz im Internet – Anforderungen und Grenzen einer Regulierung. In Neue Juristische Wochenschrift – Beilage (NJW-Beil.) 2012, pp. 98-101.

Stalla-Bourdillon, Sophie, Online monitoring, filtering, blocking… What is the difference? Where to draw the line? In Computer Law & Security Review 29 (2013), pp. 702-712.

Starosta, Justyna, Transnationaler Datenaustausch zur Terrorismusbekämpfung. In Datenschutz und Datensicherheit (DuD) 4 2010, pp. 236-239.

Stephen, James Fitzjames, Liberty, Equality, Fraternity. Originally published in 1874. This edition edited by Stuart D. Warner, Indianapolis: Liberty Fund 1993.

Stommel, Sebastian, Blockchain Ökosysteme. Identitäts- und Zugangsmanagement zur Blockchain und angedockten Ökosystemen. In Datenschutz und Datensicherheit (DuD) 1 2017, pp. 7-12.

Streinz, Rudolf, Die Rechtsprechung des EuGH zum Datenschutz. In Datenschutz und Datensicherheit (DuD) 9 2011, pp. 602-606.

Sullivan, Clare, Digital Identity: An Emergent Legal Concept (2011). University of Adelaide Press 2011.

Swire, Peter, From real-time intercepts to stored records: why encryption drives the government to seek access to the cloud. In International Data Privacy Law (IDPL), Vol. 2, No. 4, 2012, pp. 200-206.

Taylor, Veronica L. (2017), Regulatory Rule of Law. In Regulatory Theory, Foundations and applications, edited by Peter Drahos, ANU Press 2017, pp. 393-413.

Thompson, Edwina A., Misplaced Blame: Islam, Terrorism and the Origins of Hawala. In Max Planck Yearbook of United Nations Law, Volume 11, 2007, pp. 279-305.

Thomson, Judith Jarvis, The right to privacy. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Tinnefeld, Marie-Theres, Sapere Aude! Über Informationsfreiheit, Privatheit und Raster. In Neue Juristische Wochenschrift (NJW) 2007, pp. 625-630.

Tinnefeld, Marie-Theres, Privatheit als Voraussetzung menschenrechtlicher Freiräume? In Datenschutz und Datensicherheit (DuD) 9 2011, pp. 598-601.

Tolani, Madeleine, Existiert in Deutschland ein Bankgeheimnis? Das Bankgeheimnis gegenüber dem Staat unter Berücksichtigung der jüngsten gesetzlichen Veränderungen. In Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2007, pp. 275-281.

Tracfin, Unit for intelligence processing and action against illicit financial networks, Annual Report 2015. Available online at https://www.economie.gouv.fr/files/ra-ang-tracfin-2015.pdf

Tranberg, Charlotte Bagger, Proportionality and data protection in the case law of the European Court of Justice. In International Data Privacy Law (IDPL), Vol. 1, No. 4, 2011, pp. 239-248.

Tridimas, Takis, Proportionality in European Community Law: Searching for the Appropriate Standard of Scrutiny. In: The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart 1999.

Trstenjak, Verica and Beysen, Erwin, Das Prinzip der Verhältnismäßigkeit in der Unionsrechtsordnung, Europarecht (EuR) 2012, 265-285.

Trüg, Gerson, Die Reform der strafrechtlichen Vermögensabschöpfung. In Neue Juristische Wochenschrift (NJW) 2017, pp. 1913-1918.

Tschorsch, Florian and Scheuermann, Björn, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. In IEEE Communications Surveys & Tutorials, thirdquarter 2016, pp. 2084 – 2123.

Tzanou, Maria, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. In International Data Privacy Law (IDPL), Vol. 3, No. 3, 2013, pp. 88-99.

Uerpmann-Wittzack, Robert and Jankowska-Gilberg, Magdalena, Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet. In MultiMedia und Recht (MMR) 2008, pp. 83-89.

Ufer, Frederic, Die Verifikation von Kundendaten über den neuen § 111 TKG. Was Prepaid-Mobilfunknutzer mit der Bekämpfung des internationalen Terrorismus zu tun haben. In MultiMedia und Recht (MMR) 2017, pp. 83-88.

United Nations Office on Drugs and Crime UNODC, Money-Laundering and Globalization (no date), available at http://www.unodc.org/unodc/en/money-laundering/globalization.html

United Nations High Commissioner for Human Rights, The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. Human Rights Council, Twenty-seventh session, Agenda items 2 and 3, A/HRC/27/37, 30 June 2014.

United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Promotion and protection of human rights: implementation of human rights instruments. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN General Assembly, Sixty-ninth session, Agenda item 68 (a), A/69/397, 23 September 2014.

Vaccani, Matteo (2009) 'Alternative Remittance Systems and Terrorism Financing', Wold Bank Working Paper No. 180

Van Alsenoy, Brendan and Koekkoek, Marieke, Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'. In International Data Privacy Law (IDPL), Vol. 5, No. 2, 2015, pp. 105-120.

Van de Bunt, Henk, A case study on the misuse of Hawala banking. In International Journal of Social Economics, Vol. 35 Issue 9 2008, pp. 691-702.

Van der Sloot, Bart, Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. In International Data Privacy Law (IDPL), Vol. 4, No. 4, 2014, pp. 307-325.

Van Hout, Marie Claire and Bingham, Tim, Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. In International Journal of Drug Policy 25 (2014), pp. 183-189.

Vandezande, Niels, Identification numbers as pseudonyms in the EU public sector. In European Journal of Law and Technology, Vol. 2, No. 2, 2011.

Vardi, Noah, Bit by Bit: Assessing the Legal Nature of Virtual Currencies. In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 55-71.

Vlcek, William, Development vs. Terrorism: Money Transfers and EU Financial Regulations in the UK. In The British Journal of Politics and International Relations 2008, Vol. 10, pp. 286-302.

Vlcek, William, Securitizing Money to Counter Terrorist Finance: Some Unintended Consequences for Developing Economies. In International Studies Perspectives 16, 2015, pp. 406-422.

Wachter, Sandra and Mittelstadt, Brent and Floridi, Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. In International Data Privacy Law (IDPL), Vol. 7, No. 2, 2017, pp. 76-99.

Wahlquist, Calla, Gillian Triggs: Australian law has fallen prey to 'isolation and exceptionalism'. The Guardian, Wednesday 27 September 2017 10.44 BST, https://www.theguardian.com/australia-news/2017/sep/27/gillian-triggs-australian-law-has-fallen-prey-to-isolation-and-exceptionalism

Walden, Ian, Anonymising Personal Data under European Law. In: Nicoll, C and Prins, J.E.J., and van Dellen, M.J.M. (eds.), Digital Anonymity and the Law – Tensions and Dimensions. Information Technology & Law Series, Asser Press, The Hague 2003, pp. 147-159.

Waldron, Jeremy, Security and Liberty: The Image of Balance. In The Journal of Political Philosophy: Volume 11, Number 2, 2003, pp. 191–210.

Walker, Vivian, Prosecuting money launderers: does the prosecution have to prove the predicate offence? In Criminal Law Review 2009, 8, pp. 571-575.

Warde, Ibrahim, The War on Terror, Crime and the Shadow Economy in the MENA Countries. In Mediterranean Politics 12:2, 2007, pp. 233-248.

Warren, Samuel D. and Brandeis, Louis Dembitz, The Right to Privacy. In Harvard Law Review, Vol. IV, No. 5, December 15, 1890. Available at Project Gutenberg at http://www.gutenberg.org/ebooks/37368

Wassesrstrom, Richard A., Privacy – Some arguments and assumptions. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Waterman, K. Krasnow and Bruening, Paula J., Big Data analytics: risks and responsibilities. In International Data Privacy Law (IDPL), Vol. 4, No. 2, 2014, pp. 89-95.

Weber, Beat, Can Bitcoin Compete with Money? (October 20, 2013). In Journal of Peer Production 4 (2014). Available at SSRN: http://ssrn.com/abstract=2483867

Webster, C. William R., Surveillance as X-ray: Understanding the Surveillance State. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 14-28.

Wehlau, Andreas and Lutzhöft, Niels, Grundrechte-Charta und Grundrechts-Checkliste – eine dogmatische Selbstverpflichtung der EU-Organe. In Europäische Zeitschrift für Wirtschaftsrecht (EUZW) 2012, pp. 45-50.

Weichert, Thilo, Bürgerrechtskonforme Bekämpfung der Computerkriminalität. In Datenschutz und Datensicherheit (DuD) 8 2007, pp. 590-594..

Weichert, Thilo, Big Data, Gesundheit und der Datenschutz. In Datenschutz und Datensicherheit (DuD) 12 2014, pp. 831-838.

Weichert, Thilo, Führungsaufgabe „Datenschutz" bei Banken. In Datenschutz und Datensicherheit (DuD) 1 2015, pp. 16-20.

Weichert, Thilo, „Sensitive Daten" revisited. In Datenschutz und Datensicherheit (DuD) 9 2017, pp. 538-543.

Weigell, Jörg und Görlich, Michael, (Selbst-)Geldwäsche: Strafbarkeitsrisiko für steuerliche Berater? In Deutsches Steuerrecht (DStR) 2016, 2178.

Wensink, Wim, et al., The European Union's Policies on Counter-Terrorism Relevance, Coherence and Effectiveness, Study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf

Westin, Alan F., The origins of modern claims to privacy. In: Ferdinand D. Schoeman (ed.), Philosophical Dimensions of Privacy – An Anthology. Cambridge 1984.

Westin, Alan F., Social and Political Dimensions of Privacy. In Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 431-453.

Wheatley, Joseph, Ancient Banking, Modern Crimes: How Hawala secretly transfers the Finances of Criminals and thwarts existing Laws. In University of Pennsylvania Journal of International Economic Law 2005, pp. 347-378.

White, Lawrence H., The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-Gold (March 10, 2014). GMU Working Paper in Economics No. 14-06. Available at SSRN: http://ssrn.com/abstract=2406983 or http://dx.doi.org/10.2139/ssrn.2406983

Wieczorek, Mirko Andreas, Informationsbasiertes Persönlichkeitsrecht. Überlegungen zur Restauration des Persönlichkeitsschutzes im Internetzeitalter. In Datenschutz und Datensicherheit (DuD) 7 2011, pp. 476-481.

Wigoutschnigg, Raphael, Anonymisierungsprotokolle. In Datenschutz und Datensicherheit (DuD) 7 2012, pp. 515-519.

Winer, Jonathan M. and Roule, Trifin J., Fighting Terrorist Finance. In Survival, Global Politics and Strategy, 44:3, 2002, pp. 87-104.

Wolf, Redmar A., Virtual Currencies, M-Payments and VAT: Ready for the Future? In: Gimigliano, Gabriella (ed.), Bitcoin and Mobile Payments, Constructing a European Union Framework. Palgrave Studies in Financial Services Technology, London 2016, pp. 231-249.

Worms, Christoph and Gusy, Christoph, Verfassung und Datenschutz. Das Private und das Öffentliche in der Rechtsordnung. In Datenschutz und Datensicherheit (DuD) 2 2012, pp. 92-99.

Wright, David and Friedewald, Michael and Gellert, Raphaël, Developing and testing a surveillance impact assessment methodology. In International Data Privacy Law (IDPL), Vol. 5, No. 1, 2015, pp. 40-53.

Yngvesson, Susanne Wigorts, To See the World as it Appears: The Look, the Camera and the Flesh. In C. William R. Webster, Gemma Galdon Clavell, Nils Zurawski, Kees Boersma, Bence Ságvári, Christel Backman, and Charles Leleux (eds.), Living in Surveillance Societies: 'The State of Surveillance', Proceedings of LiSS Conference 3, 2012, pp. 314-323.

Zeidler, Irrungen und Wirrungen – Die unzulängliche staatliche Regulierung im Geldwäscherecht. In Corporate Compliance Zeitschrift (CCZ) 2014), pp. 105-113.

Zentes, Uta and Wybitul, Tim, Interne Sicherungsmaßnahmen und datenschutzrechtliche Grenzen bei Kreditinstituten sowie bei anderen Instituten des Finanzwesens – Neue Anforderungen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen. In Corporate Compliance Zeitschrift (CCZ) 2011, pp. 90-95.

Ziebarth, Wolfgang, Grundrechtskonforme Gestaltung der Vorratsdatenspeicherung. Überlegungen zu einer europa-, verfassungs- und datenschutzrechtskonformen Umsetzung. In Datenschutz und Datensicherheit (DuD) 1 2009, pp. 25-32.

Zikesch, Philipp and Reimer, Bernd, Datenschutz und präventive Korruptionsbekämpfung – kein Zielkonflikt. In Datenschutz und Datensicherheit (DuD) 2 2010, pp. 96-98.

# V

# English Summary

This PhD thesis takes a closer look at the conflict between the right to privacy on the one hand and the effective investigation into serious crime on the other hand. Law enforcement authorities have the task of preventing and investigating crimes such as money laundering, and the protection of the fundamental right to privacy ensures that the authorities do not encroach too much on the fundamental rights and freedoms of individuals while fighting these crimes. There is, therefore, a clash between the interests of law enforcement authorities in gathering information helping them in their fight against crime, and the interest of individuals in protecting their privacy.

The main research question which this thesis seeks to answer is whether the balance struck between the right to privacy and the interest in effective law enforcement in the Anti-money laundering Directive (EU) 2015/849 respects the principle of proportionality.

Anti-money laundering legislation originated in the 1970s in the United States and in Europe, slowly evolving into an international network of numerous national and international instruments determining the approach to money laundering and terrorist financing which is now followed in almost all countries across the world. According to this approach, financial service providers of all descriptions are involved in the detection of and investigation into potential money laundering operations. The obligations falling onto those services providers are fourfold: in the first place, all customers must be identified and their identities verified. Secondly, all transactions must be monitored by the service provider in order to be able to filter out any suspicious transactions. If any suspicious activity is detected, the obliged entity must in the third place forward this information to the national Financial Intelligence Unit (FIU) and comply with requests for information if the FIU requests any data. In the fourth place, information identifying the customer and transaction records must be retained for five years after the end of the business relationship. This anti-money laundering regime is rigorously applied, and covers all participants in the financial service industry: in principle, all providers and all customers are covered. The scope of the anti-money laundering regime is nearly unparalleled.

In principle, therefore, the anti-money laundering approach covers all means of financial transactions, including alternative financial transaction systems. Virtual

currencies and alternative value transfer services such as the Hawala system serve as examples in this context. Virtual currency systems, the first group of transaction systems that are addressed in this thesis, are still a new system for financial transactions, usually based on a peer-to-peer system and cryptography. Bitcoin serves as a primary example. Its open structure eliminates the need for a central authority such as a bank in order to reliably transfer funds. The second group of alternative transaction systems that is addressed in this thesis is that of informal value transfer services, particularly Hawala. Hawala is a network of service providers transferring funds in such a way that the funds do not move physically. Hawala is fast, cost-effective, secure, and culturally convenient to its users, who are in Europe often members of the expatriate communities from countries in which Hawala is the dominant financial service.

The Anti-money laundering Directive is unable to cover alternative systems for financial transactions in a similarly comprehensive way as it does the conventional banking sector. Virtual currencies elude the anti-money laundering approach by lacking a central authority which could be obliged to apply the anti-money laundering measures. Virtual currencies are in fact not an institution but in essence simply a computer programme run by a network of individuals around the world. Therefore, the system itself is not covered. The only aspect of virtual currencies currently already covered by the Directive are service providers connecting to the system, such as virtual currency exchange services. Those service providers can already be classified as obliged entities under the terms of the fourth Anti-money laundering Directive. The upcoming fifth Anti-money laundering Directive explicitly covers these service providers as obliged entities, creating legal certainty in this respect. Users can, however, use virtual currencies without making use of these services, or they may turn to service providers located in a state outside of the European Union with weak anti-money laundering oversight mechanisms. This limits the potential benefit of the coverage of those systems by European law for the purposes of anti-money laundering. The coverage of decentral virtual currency systems like Bitcoin by anti-money laundering legislation is therefore incomplete.

Hawala is at once different and similar in this case. The Hawala system is in essence a large network of interconnected persons, very similar to virtual currencies, except that hawaladars can easily offer their services without a sophisticated

technological infrastructure. Hawaladars in Europe usually cater first and foremost to the members of the expatriate communities they themselves belong to, offering their services to people wishing to send remittances to their home country. The very simple nature of the service they provide allows them a large degree of flexibility and independence, and makes them resilient to attempts at regulation. The fact that funds need not move physically, combined with the fact that hawaladars generally operate underground and in noncompliance with the applicable financial regulation, also causes the incomplete coverage of this system. The activities of a hawaladar are difficult to detect by the authorities and even more difficult to sustainably prevent, considering the great demand for the services of hawaladars. Therefore, it can be stated that the anti-money laundering approach only really matches the parts of the financial sector for which it was designed, leaving large gaps in oversight over alternative services.

It has already been outlined that the anti-money laundering legislation is essentially based on data processing on a large scale. In this way, it potentially conflicts with the rights to privacy and data protection. The rights to privacy and data protection are supporting pillars of a free and democratic society, enshrined in article 8 ECHR and articles 7 and 8 of the Charter of Fundamental Rights of the European Union. These rights protect the individual from intrusions into his or her private life and from illegitimate processing of his or her personal data. In order to ensure the protection of these rights, the data subject is endowed with a number of rights under the General Data Protection Regulation (GDPR) and, to a somewhat lesser extent, the Police and Criminal Justice Authorities Directive. These instruments add details to the protection of the rights to privacy and data protection by codifying a number of rights of the data subjects, fundamental principles for the protection of data, and other formal and material rules concerning data processing.

In essence, all data relating to an identified or identifiable person is protected under the data protection rules. Anonymous data, on the other hand, is in principle excluded from the scope of protection of the right to data protection. This definition, however, raises the question what the concept of identity really means.

The concept of identity is complex, and it is defined very differently in different scientific disciplines. According to the sociological model used in this thesis,

an individual distinguishes between a personal identity and a social identity. A personal identity is formed by the personal attributes on which an individual places particular emphasis, while a social identity is formed along the lines of how the rest of society perceives an individual. In legal terms, the focus of identity in the first place lies on the question how one individual can be distinguished from all other individuals. While the state may achieve this task by assigning each resident a personal identification number, it may also be achieved by the combination of name and date and place of birth or other identifiers. At the same time, other identifiers may serve the same purpose of singling an individual out from the rest of the group, particularly by third parties. Where an individual is identified or identifiable, the data protection legislation is applicable, with all the rights, restrictions, and principles contained therein. Where an individual is anonymous, on the other hand, the data protection legislation is in principle not applicable. Data is anonymous when the data cannot be linked to an identified or identifiable natural person. However, in many instances even anonymised data can, where the anonymization process was not thorough enough, be linked to an identifiable person. There is so much data available on identified and identifiable persons already, that the possibility of linking previously anonymous data to an identified or identifiable individual can hardly be excluded.

The identity of an individual is also always involved in financial transactions. The Anti-money laundering Directive explicitly forbids anonymous accounts, and demands that all obliged entities fully identify all of their customers. The anti-money laundering framework speaks of identifying customers in a legal sense, that is, customers must prove their identity by means of an official document uniquely identifying them. In addition, the aspects of personal and social identity are also closely connected to the measures contained in the Directive. When a customer begins a long-term business relationship with a service provider, such as is the case when a customer opens a bank account with a credit institution, the service provider will quickly accumulate a large amount of personal information about this customer. The personal information is here not only limited to identifying information as contained in one's official identity document, but also information pertaining to other aspects of a person's identity. In this way, the transaction history of a bank customer will often allow for accurate inferences to be drawn concerning the customer's personal circumstances, including, under certain conditions, his or her sexual preference, religious conviction, political opinion,

and many other aspects. The transactions of the customer are at the same time subject to anti-money laundering measures, which equally affect all transactions revealing sensitive personal information.

The concept of identity also comes into play when a customer proves his or her identity, and when the intimate connection of identity with the notion of privacy is considered. For instance, one's identity is to a large extent shaped by traits which are directly linked to categories of data which are considered sensitive. An individual's sexual orientation, medical condition, and religious beliefs are often large factors in their identity, but information about these factors is considered sensitive and should in principle not be processed. Information relating to these intimate and sensitive aspects of an individual's identity can, however, often also be found in the customer's transaction history.

The impact of an individual's identity on the choice of a financial transaction system should not be underestimated. Some members of the population face difficulties when a proof of their identity is demanded. In addition to that point, a person's social and personal identity can play a major role in their choice for a transaction system. There are persons who avoid the conventional banking sector and instead decide to opt for a different transaction system. Religious and ideological views and concerns can play a big role in the customer's choice for virtual currencies or informal value transfer services.

This direct connection between the anti-money laundering framework and the customer's identity, privacy and personal data, lies at the core of this thesis. The connection between the legitimate interest in protecting the customer's identity and privacy on the one hand, and the erosion of this protection by the anti-money laundering measures on the other hand is strong, as the identity of the customer influences not only his or her choices, but is also reflected in his or her behaviour, including in financial transactions. At the same time, there are hardly any options for the customer to protect his or her identity when using financial services. Therefore, one of the main conclusions reached in this thesis is that there is insufficient protection of privacy and identity in financial transactions.

What precisely would be sufficient protection is determined with the help of the principle of proportionality as applied by the Court of Justice of the European

Union (CJEU) and the European Court of Human Rights (ECtHR). In essence, the principle of proportionality demands that any measure should not interfere with the rights of the population more than is necessary in order to achieve the aim pursued by that measure. The CJEU and ECtHR apply the principle slightly differently. The CJEU applies a test of three steps. It asks first, whether a measure is suitable to achieve the aim it pursues, secondly, whether the measure does not go beyond what is necessary to achieve the aim, and thirdly, whether the conflicting interests involved are properly balanced. The ECtHR, in contrast, has not yet chosen to develop a standard test. The case law of the ECtHR generally concentrates on the applicable safeguards accompanying a measure, and the 'relevant and sufficient reasons' given by the lawmaker in order to show that a measure is necessary in a democratic society and addressing 'a pressing social need'. When applied to a given measure, however, the different tests of the CJEU and the ECtHR generally yield the same outcome.

With the help of the foregoing insights, the main research question of this thesis is addressed. This question is whether the anti-money laundering measures as currently applied across Europe properly respect the rights to privacy and data protection. According to article 52 of the Charter of Fundamental Rights of the European Union, a measure is in accord with human rights only if it is provided for by law, respects the essence of the right, and if the intensity of the interference of the measure with human rights is proportionate to the aim it pursues. The proportionality assessment lays at the core of the assessment.

The measures of the Anti-money laundering Directive interfere with the privacy of individuals in several different ways. Individuals are identified when the obligations of the Anti-money laundering Directive are triggered, and copies of the documents are retained by the service provider for five years after the end of the business relationship between the customer and the service provider. Furthermore, all transaction are monitored by the service provider, and a transaction history is also retained for five years after the end of the business relationship. The processing and retention of data constitute further interferences. When a transaction appears suspicious, the Financial Intelligence Unit is informed of it. The transmission of data to the FIU is another interference. The inclusion of customer information in central databases should also be seen as an interference. Considering that almost every inhabitant of the European Union fundamentally depends on financial

services to be able to participate in society, and that the rules of the Directive therefore comprehensively affect the entire European population, the author argues that the interference of the Directive should be considered particularly serious.

It may be argued that the anti-money laundering measures pursue the legitimate aim of preventing and facilitating the detection and investigation into serious crime and are therefore justified. However, the interest of the population in protecting their privacy and personal data is equally justified. Therefore, it is particularly important that the measures do not go beyond what is necessary, and that a balance is struck between the conflicting interests.

The design of the measures raises some concerns about their compatibility with the rights to privacy and data protection. There are several concerns that can be raised in this context, the most striking of which are the mass surveillance character of the measures, the lack of safeguards for sensitive categories of data, the excessive retention periods, and the lack of procedural safeguards ensuring the protection of the rule of law. Based on the existing case law of the CJEU, it can be argued that the measures of the Directive go beyond what is necessary to achieve the aim pursued. The measures cut too deeply into the privacy of customers to be considered in accord with the principle of proportionality. The rights to privacy and data protection are not properly balanced with the interest in facilitating the fight against serious crime. Therefore, the measures of the Anti-money laundering Directive do not properly respect the principle of proportionality.

The CJEU is exclusively competent to rule on the proportionality of a European directive. In the event that the Anti-money laundering Directive is challenged before the Court, and if the CJEU agrees with the assessment made in this thesis, the Court will invalidate the Anti-money laundering Directive. The anti-money laundering measures would have to be redrafted with the consideration due to the proper respect for human rights. This would essentially cause a shift to the warrant-system, according to which law enforcement authorities must identify a suspect and obtain a judicial authorisation for the access to specific sets of data held by certain service providers. This obligation to obtain a warrant would grant data subjects the higher level of protection of judicial review. The quick-freeze system

may also be explored as a potential approach in order to ensure the retention of certain data sets.

Finally, it should be mentioned that a careful examination of the proportionality test shows one serious shortcoming of the test: it can only be applied to one legal instrument or measure at a time, and that only after a lengthy and costly legal procedure. It does not allow for the assessment of the cumulative effect of two or more measures. It is the cumulative effect, however, which will often have a particularly negative effect on the privacy of individuals.

Against this background, this thesis also engages with the discussion of the question whether the approach currently applied to the review of the legality of surveillance measures and other intrusions into the privacy of the population is an adequate mechanism for the protection of the essence of the rights to privacy and data protection. It is clear that the mechanisms for the protection of the rights to privacy and personal data are not suitable to protect data subjects from dangers presented by Big Data projects, mass surveillance, and cleverly drafted legislation.

A holistic view of the entire landscape of the surveillance measures with which a data subject is confronted is therefore indispensable in order to ensure the proper protection of the rights of the data subject and preventing the gradual hollowing-out of the rights to privacy and data projection by the multitude of existing interferences. While each interference with the rights of the data subject may be justified and proportionate when viewed individually and in isolation, the combination of these measures may be well capable of interfering with the essence of the rights to privacy and data protection. The lack of meaningful protection against this danger is intolerable and should be remedied on the European level without delay.

# VI

# Nederlandstalige Samenvatting

Dit proefschrift gaat nader in op het conflict tussen het recht op privacy enerzijds en effectief onderzoek van criminaliteit anderzijds. Wetshandhavingsinstanties hebben de taak misdrijven zoals het witwassen van geld te voorkomen en te onderzoeken, en de bescherming van het grondrecht op privacy zorgt ervoor dat de wetshandhavingsinstanties tijdens de bestrijding van deze misdrijven niet te veel inbreuk maken op de fundamentele rechten en vrijheden van personen. Er bestaat daarom een conflict tussen het belang van wetshandhavingsautoriteiten bij het verzamelen van informatie en het belang van individuen bij het beschermen van hun privacy.

De belangrijkste onderzoeksvraag die dit proefschrift centraal stelt, is of het evenwicht tussen het recht op privacy en het belang van effectieve wetshandhaving in de vierde anti-witwasrichtlijn (EU) 2015/849 in overeenstemming is met het evenredigheidsbeginsel.

Anti-witwaswetgeving is ontstaan in de jaren 70 in de Verenigde Staten en in Europa, langzaam evoluerend naar een internationaal netwerk van talrijke nationale en internationale instrumenten die de aanpak bepalen tegen het witwassen van geld en terrorismefinanciering, die nu wordt gevolgd in bijna alle landen over de hele wereld. Volgens deze aanpak zijn financiële dienstverleners van alle soorten en maten betrokken bij het voorkomen, melden en opsporen van mogelijke witwasoperaties. Er rusten vier verplichtingen op deze dienstverleners: in de eerste plaats moeten alle klanten worden geïdentificeerd en moeten hun identiteiten worden geverifieerd. Ten tweede moeten alle transacties door de serviceprovider worden gemonitord om verdachte transacties te kunnen filteren. Als een verdachte activiteit wordt gedetecteerd, moet de verplichte entiteit in de derde plaats deze informatie doorsturen naar de nationale Financial Intelligence Unit (FIU) en voldoen aan verzoeken om informatie als de FIU daarom vraagt. In de vierde plaats moet informatie die de klant en transactiegegevens identificeert tot gedurende vijf jaar na het einde van de zakelijke relatie worden bewaard. Dit anti-witwasregime wordt rigoureus toegepast en is van toepassing op alle deelnemers aan de financiële dienstverlening: in principe zijn alle aanbieders en alle klanten gedekt. De reikwijdte van het anti-witwasregime is bijna ongeëvenaard.

In principe omvat de anti-witwaswetgeving derhalve alle vormen van financiële transacties, inclusief alternatieve systemen voor financiële transacties. Virtuele

valuta en alternatieve waardeoverdrachtsdiensten zoals het Hawala-systeem dienen in dit verband als voorbeelden. Virtuele valutasystemen, de eerste groep transactiesystemen die in dit proefschrift wordt behandeld, vormen nog steeds een nieuw systeem voor financiële transacties, meestal gebaseerd op een peer-to-peer-systeem en cryptografie. Bitcoin dient als een primair voorbeeld. De open structuur elimineert de noodzaak voor een centrale autoriteit zoals een bank om op betrouwbare wijze geld over te maken. De tweede groep alternatieve transactiesystemen die in dit proefschrift wordt behandeld, is die van informele diensten voor waardeoverdracht, met name Hawala. Hawala is een netwerk van serviceproviders die fondsen zodanig overdragen dat het geld niet fysiek wordt verplaatst. Hawala is snel, kosteneffectief, veilig en cultureel handig voor zijn gebruikers, die in Europa vaak lid zijn van emigrantengemeenschappen uit landen waarin Hawala de dominante financiële service is.

De anti-witwasrichtlijn kan alternatieve systemen voor financiële transacties niet op een even omvattende manier dekken als de conventionele banksector. Virtuele valuta ontglippen de aanpak tegen het witwassen van geld doordat er een centrale autoriteit ontbreekt die zou kunnen worden verplicht de anti-witwasmaatregelen toe te passen. Virtuele valuta zijn in feite geen instellingen, maar in essentie gewoon computerprogramma's die worden gerund door netwerken van individuen over de hele wereld. Daarom is het systeem zelf niet gedekt. Het enige aspect van virtuele valuta dat momenteel wel onder de richtlijn valt, zijn dienstverleners zoals virtuele wisselkantoren. Die dienstverleners kunnen al worden aangemerkt als verplichte entiteiten onder de voorwaarden van de vierde richtlijn tegen het witwassen van geld. De komende vijfde richtlijn noemt deze dienstverleners expliciet en creëert hierdoor rechtszekerheid. Gebruikers kunnen virtuele valuta echter gebruiken zonder gebruik te maken van deze services, of ze kunnen zich wenden tot serviceproviders in een staat met zwakke anti-witwastoezichtmechanismen. Dit beperkt het potentiële voordeel van de dekking van die systemen door Europese wetgeving met het oog op het witwassen van geld. De dekking van decentrale virtuele valutasystemen zoals Bitcoin door wetgeving tegen het witwassen van geld is daarom onvolledig.

Hawala is in dit geval zowel verschillend als vergelijkbaar. Het Hawala-systeem is in wezen een groot netwerk van onderling verbonden personen, zeer vergelijkbaar met virtuele valuta, behalve dat hawaladars hun diensten eenvoudig

kunnen aanbieden zonder een geavanceerde technologische infrastructuur. Hawaladars in Europa verzorgen meestal eerst en vooral de leden van de emigrantengemeenschappen waartoe zij zelf behoren door hun diensten aan te bieden aan mensen die overschrijvingen naar hun eigen land willen doen. De zeer eenvoudige aard van de geboden service biedt een grote mate van flexibiliteit en onafhankelijkheid en maakt het systeem weerbaarder tegen pogingen tot regulering. Het feit dat fondsen niet fysiek hoeven te bewegen, gecombineerd met het feit dat hawaladars over het algemeen ondergronds opereren en niet voldoen aan de relevante financiële regelgeving veroorzaakt ook de onvolledige dekking van dit systeem. De activiteiten van een hawaladar zijn moeilijk te detecteren door de autoriteiten en zelfs nog moeilijker om duurzaam te voorkomen, gezien de grote vraag naar de diensten van hawaladars. Daarom kan worden gesteld dat de aanpak tegen het witwassen van geld alleen echt overeenkomt met de delen van de financiële sector waarvoor deze is ontworpen, waardoor er grote gaten zijn in het toezicht op alternatieve diensten.

Er is al geschetst dat de anti-witwaswetgeving hoofdzakelijk gebaseerd is op gegevensverwerking op grote schaal. Hierdoor is het mogelijk in strijd met de rechten op privacy en gegevensbescherming. De rechten op privacy en gegevensbescherming zijn ondersteunende pijlers van een vrije en democratische samenleving, verankerd in artikel 8 EVRM en artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Deze rechten beschermen het individu tegen inbreuken op zijn of haar privéleven en tegen onrechtmatige verwerking van zijn of haar persoonlijke gegevens. Om de bescherming van deze rechten te waarborgen, beschikt de betrokkene over een aantal rechten op grond van de Algemene Verordening Gegevensbescherming (AVG) en, in iets mindere mate, de politie- en strafrechtelijke autoriteitenrichtlijn. Deze instrumenten voegen details toe aan de bescherming van de rechten op privacy en gegevensbescherming door een aantal rechten van de betrokkenen te codificeren, fundamentele beginselen voor de bescherming van gegevens en andere formele en materiële regels betreffende gegevensverwerking.

In essentie worden alle gegevens met betrekking tot een geïdentificeerde of identificeerbare persoon beschermd. Anonieme gegevens daarentegen zijn in beginsel uitgesloten van de bescherming van het recht op gegevensbescherming. Deze definitie roept echter de vraag op wat het identiteitsbegrip eigenlijk betekent.

Het concept van identiteit is complex en het is heel verschillend gedefinieerd in diverse wetenschappelijke disciplines. Volgens het model dat in dit proefschrift wordt gebruikt, maakt een individu onderscheid tussen een persoonlijke identiteit en een sociale identiteit. Een persoonlijke identiteit wordt gevormd door de persoonlijke eigenschappen waar een persoon bijzondere nadruk op legt, terwijl een sociale identiteit is gebaseerd op hoe de rest van de samenleving een individu waarneemt. In juridisch opzicht ligt de focus van identiteit in de eerste plaats op de vraag hoe een persoon kan worden onderscheiden van alle andere individuen. Hoewel de staat deze taak kan vervullen door aan elke bewoner een persoonlijk identificatienummer toe te wijzen, kan deze ook worden bereikt door de combinatie van naam en geboorteplaats en -datum of andere identificatiegegevens. Tegelijkertijd kunnen andere identificatiegegevens hetzelfde doel dienen om een persoon van de rest van de groep te onderscheiden, met name door derden. Wanneer een persoon geïdentificeerd of identificeerbaar is, is de wetgeving inzake gegevensbescherming van toepassing, met alle rechten, restricties en principes die erin zijn vervat. Wanneer gegevens anoniem zijn, is de wetgeving inzake gegevensbescherming in beginsel niet van toepassing. Gegevens zijn anoniem wanneer de gegevens niet kunnen worden gekoppeld aan een geïdentificeerde of identificeerbare natuurlijke persoon. In veel gevallen kunnen echter zelfs geanonimiseerde gegevens, waar het anonimiseringsproces niet grondig genoeg was, worden gekoppeld aan een identificeerbare persoon. Er is al zoveel data beschikbaar over geïdentificeerde en identificeerbare personen, dat de mogelijkheid om op zich anonieme gegevens te koppelen aan een geïdentificeerde of identificeerbare persoon nauwelijks kan worden uitgesloten.

De identiteit van een persoon is ook altijd betrokken bij financiële transacties. De anti-witwasrichtlijn verbiedt expliciet anonieme accounts en eist dat alle meldingsplichtige entiteiten al hun klanten volledig identificeren. Het kader voor het witwassen van geld spreekt van het identificeren van klanten in juridische zin, dat wil zeggen dat klanten hun identiteit moeten bewijzen door middel van een officieel document dat hen op unieke wijze identificeert. De aspecten van persoonlijke en sociale identiteit hangen echter ook nauw samen met de maatregelen in de richtlijn. Wanneer een klant een zakelijke relatie met een serviceprovider begint, zoals wanneer een klant een bankrekening bij een kredietinstelling opent, verzamelt de serviceprovider snel een grote hoeveelheid persoonlijke gegevens over deze klant. De persoonlijke informatie is hier niet alleen beperkt tot het

identificeren van informatie zoals vervat in het officiële identiteitsbewijs, maar ook informatie die betrekking heeft op andere aspecten van iemands identiteit. Op deze manier kan de transactiegeschiedenis van een bankklant vaak leiden tot nauwkeurige conclusies over de persoonlijke omstandigheden van de klant, waaronder, onder bepaalde voorwaarden, zijn seksuele voorkeur, religieuze overtuiging, politieke mening en vele andere aspecten. De transacties van de klant zijn tegelijkertijd onderworpen aan maatregelen tegen het witwassen van geld, die eveneens van invloed zijn op alle transacties die gevoelige persoonlijke informatie onthullen.

Hierin ligt de directe verbinding van identiteit met privacy. Iemands identiteit wordt bijvoorbeeld sterk beïnvloedt door eigenschappen die direct gekoppeld zijn aan categorieën van gegevens van gevoelige aard. De seksuele oriëntatie, medische toestand en de religieuze overtuigingen van een persoon zijn vaak bepalende factoren voor iemands identiteit, maar informatie over deze factoren wordt als bijzonder gevoelig beschouwd en mag in principe niet worden verwerkt. Informatie met betrekking tot deze intieme en gevoelige aspecten van de identiteit van een persoon kan echter vaak ook worden gevonden in de transactiegeschiedenis van de klant.

De impact van de identiteit van een individu op de keuze van een financieel transactiesysteem moet ook niet worden onderschat. Sommige leden van de bevolking kunnen te maken krijgen met ernstige moeilijkheden wanneer een bewijs van hun identiteit wordt geëist. In aanvulling hierop kan de sociale en persoonlijke identiteit van een persoon een belangrijke rol spelen bij zijn of haar keuze voor een transactiesysteem. Er zijn personen die de conventionele banksector mijden en in plaats daarvan kiezen voor een ander transactiesysteem. Religieuze en ideologische opvattingen kunnen een grote rol spelen in de keuze van de klant voor virtuele valuta of een informele dienst zoals Hawala.

De directe verbinding tussen het anti-witwaskader en de identiteit, privacy en persoonlijke gegevens van de klant, vormt de kern van dit proefschrift. Het verband tussen het legitieme belang bij het beschermen van de identiteit en privacy van de klant, en de uitholling van deze bescherming door de maatregelen tegen het witwassen van geld is sterk, omdat de identiteit van de klant niet alleen zijn of haar keuzes beïnvloedt, maar ook wordt weerspiegeld in zijn of haar gedrag, ook met

betrekking tot financiële transacties. Tegelijkertijd zijn er nauwelijks mogelijkheden voor de klant om zijn of haar identiteit te beschermen bij het gebruik van financiële diensten. Daarom is één van de belangrijkste conclusies in dit proefschrift dat er onvoldoende bescherming is tegen privacy- en identiteitsproblemen bij financiële transacties.

Wat voldoende bescherming is, wordt bepaald met behulp van het evenredigheidsbeginsel zoals toegepast door het Hof van Justitie van de Europese Unie (HvJEU) en het Europees Hof voor de Rechten van de Mens (EHRM). In wezen vereist het evenredigheidsbeginsel dat elke maatregel de rechten van de bevolking niet meer mag verstoren dan noodzakelijk is om het met die maatregel nagestreefde doel te bereiken. Het HvJEU en het EHRM passen het beginsel enigszins anders toe. Het HvJEU hanteert een test van drie stappen. Eerst wordt onderzocht of een maatregel geschikt is om het nagestreefde doel te bereiken, ten tweede, of de maatregel niet verder gaat dan wat nodig is om het doel te bereiken, en ten derde, of de tegenstrijdige belangen in kwestie in evenwicht zijn. Het EHRM heeft daarentegen nog niet gekozen voor het ontwikkelen van een standaardtest. De jurisprudentie van het EHRM concentreert zich over het algemeen op de toepasselijke waarborgen die gepaard gaan met een maatregel en de 'relevante en toereikende redenen' die de wetgever heeft gegeven om aan te tonen dat een maatregel noodzakelijk is om in een democratische samenleving 'een dringende sociale behoefte' aan te pakken. Wanneer ze echter op een bepaalde maatregel worden toegepast, leveren de verschillende tests van het HvJEU en het EHRM over het algemeen hetzelfde resultaat op.

Met behulp van de voorgaande inzichten wordt de belangrijkste onderzoeksvraag van dit proefschrift beantwoord. Deze vraag is of de maatregelen tegen het witwassen van geld, die momenteel in heel Europa worden toegepast, de rechten op privacy en gegevensbescherming voldoende respecteren. Volgens artikel 52 van het Handvest van de grondrechten van de Europese Unie is een op een bepaald recht inbrekende maatregel alleen in overeenstemming met de mensenrechten als de maatregel bij wet is gesteld, de wezenlijke inhoud van de rechten wordt gerespecteerd en de intensiteit van de inbreuk door de maatregel op het recht evenredig is aan het doel dat zij nastreeft. Het evenredigheidsbeginsel vormt de kern van de beoordeling.

De maatregelen van de anti-witwasrichtlijn breken op verschillende manieren in op het recht op privacy. Personen worden geïdentificeerd wanneer de verplichtingen van de anti-witwasrichtlijn van toepassing zijn en kopieën van de documenten door de dienstverlener tot gedurende vijf jaar na het einde van de zakelijke relatie tussen de klant en de dienstverlener worden bewaard. Dit is een inbreuk op het recht op privacy en het recht op gegevensbescherming. Bovendien worden alle transacties gecontroleerd door de dienstverlener en wordt een transactiegeschiedenis bewaard gedurende vijf jaar na het einde van de zakelijke relatie. De verwerking en het bewaren van deze gegevens vormen verdere inbreuken. Wanneer een transactie verdacht lijkt, wordt de financiële-inlichtingeneenheid of Financial Intelligence Unit (FIU) hiervan op de hoogte gebracht. De overdracht van gegevens naar de FIU is ook een inbreuk. Het opnemen van klantinformatie in centrale databases moet ook als een inbreuk worden beschouwd. Gezien het feit dat bijna elke inwoner van de Europese Unie fundamenteel afhankelijk is van financiële diensten om aan de samenleving te kunnen deelnemen en de maatregelen van de richtlijn daarom de gehele Europese bevolking treffen, is de auteur van mening dat de inbreuken door de maatregelen van de richtlijn als bijzonder ernstig beschouwd moeten worden.

Er kan worden betoogd dat de maatregelen ter bestrijding van het witwassen van geld het legitieme doel nastreven van het voorkomen en het vergemakkelijken van de opsporing en het onderzoek naar ernstige criminaliteit en daarom gerechtvaardigd zijn. Het belang van de bevolking bij het beschermen van hun privacy en persoonlijke gegevens is echter even gerechtvaardigd. Daarom is het bijzonder belangrijk dat de maatregelen niet verder gaan dan wat er nodig is en dat er een evenwicht wordt gevonden tussen de tegenstrijdige belangen.

Het ontwerp van de maatregelen roept enige bezorgdheid op over de verenigbaarheid ervan met het recht op privacy en het recht op gegevensbescherming. Er zijn verschillende aandachtspunten die in dit verband naar voren moeten worden gebracht, met als opvallendste het massasurveillance-karakter van de maatregelen, het ontbreken van waarborgen voor gevoelige gegevenscategorieën, de buitensporige bewaartermijnen en het ontbreken van procedurele waarborgen voor de bescherming van de rechtsstaat. Op basis van de bestaande jurisprudentie van het HvJEU kan worden gesteld dat de maatregelen van de richtlijn verder gaan dan wat nodig is om het nagestreefde doel te bereiken. De maatregelen snijden te diep in de privacy van klanten om als proportioneel te kunnen worden beschouwd.

De rechten op privacy en gegevensbescherming zijn niet goed in evenwicht met het belang om de bestrijding van zware criminaliteit te vergemakkelijken. Daarom voldoen de maatregelen van de anti-witwasrichtlijn niet voldoende aan het evenredigheidsbeginsel.

Het HvJEU is exclusief bevoegd om over de evenredigheid van een Europese richtlijn te oordelen. In het geval dat de richtlijn tegen het witwassen van geld voor het Hof wordt aangevochten en als het HvJEU het eens is met de beoordeling in dit proefschrift, zal het Hof de richtlijn tegen het witwassen van geld vernietigen. De maatregelen ter bestrijding van het witwassen van geld zouden moeten worden herschreven met inachtneming van de juiste eerbiediging van de mensenrechten. Dit zou in wezen een verschuiving veroorzaken naar een vereiste van een rechterlijke machtiging, volgens welke rechtshandhavingsinstanties een verdachte moeten identificeren en een rechterlijke machtiging moeten verkrijgen voor de toegang tot gegevens die door financiële instellingen over de verdachte zijn verzameld. Deze verplichting om een rechterlijke machtiging te verkrijgen, zou betrokkenen de hogere bescherming van rechterlijke toetsing verlenen. Het quick freeze systeem kan ook worden onderzocht als een potentiële benadering om het behoud van bepaalde gegevenssets te waarborgen.

Tot slot moet worden opgemerkt dat een zorgvuldig onderzoek van de evenredigheidstest een ernstige tekortkoming van de test aantoont: deze kan slechts op één rechtsinstrument of maatregel tegelijk worden toegepast en dit kan alleen na een langdurige en kostbare juridische procedure. De test staat niet toe dat het cumulatieve effect van twee of meer maatregelen tegelijk wordt beoordeeld. Het is echter het cumulatieve effect dat vaak bijzonder negatieve gevolgen zal hebben voor de privacy van individuen.

Tegen deze achtergrond houdt dit proefschrift ook verband met de discussie over de vraag of de huidige aanpak van de toetsing van de wettigheid van surveillancemaatregelen en andere inbreuken op de privacy van de bevolking een adequaat mechanisme is voor de bescherming van de essentie van het recht op privacy en het recht op gegevensbescherming. Het is duidelijk dat de bestaande mechanismen voor de bescherming van het recht op privacy en het recht op persoonlijke gegevens niet geschikt zijn om betrokkenen te beschermen tegen de gevaren van Big Data-projecten, massasurveillance en slim opgestelde wetgeving.

Een holistische kijk op het hele landschap van de surveillancemaatregelen waarmee een betrokkene wordt geconfronteerd, is daarom onmisbaar om de juiste bescherming van de rechten van de betrokkene te waarborgen. Op die manier kan ook de geleidelijke uitholling van het recht op privacy en het recht op gegevensbescherming door de veelheid van bestaande inbreuken voorkomen worden. Hoewel elke inmenging in de rechten van de betrokkene gerechtvaardigd en proportioneel kan zijn wanneer ze afzonderlijk worden bekeken, kan de combinatie van deze maatregelen de essentie van het recht op privacy en het recht op gegevensbescherming ernstig verstoren. Het ontbreken van een zinvolle bescherming tegen dit gevaar is onaanvaardbaar en moet onverwijld op Europees niveau worden verholpen.

*“Im Übrigen ist es nicht die Aufgabe unbescholtener Bürger, auf ihre Freiheitsrechte zu verzichten, um der Polizei ihre Arbeit zu erleichtern.“*

Ulrich Schellenberg

# Abstract

*Privacy and Identity Issues in Financial Transactions*

The research focuses on privacy and data protection, but also on the concepts of identity and anonymity, in order to shed light on the impact of the Anti-money laundering Directive from a different angle. Furthermore, alternative financial services such as virtual currencies are considered.

*The Proportionality of the Anti-money laundering Directive*

The subject of this thesis is the impact of the Anti-money laundering Directive on the fundamental right to privacy of individuals using financial services. Analysing the Directive in a very similar way to that in which the CJEU analysed the Data retention Directive, the proportionality of the anti-money laundering measures is tested.