Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy

On the Reduction of Privacy by National Authorities in Cases of National Security and Justice Matters

Vrije Universiteit

Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy

On the Reduction of Privacy by National Authorities in Cases of National Security and Justice Matters

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad Doctor aan
de Vrije Universiteit Amsterdam,
op gezag van de rector magnificus
prof.dr. V. Subramaniam,
in het openbaar te verdedigen
ten overstaan van de promotiecommissie
van de Faculteit der Rechtsgeleerdheid
op vrijdag 10 juni 2016 om 9.45 uur
in de aula van de universiteit,
De Boelelaan 1105
1081 HV Amsterdam

door

Robert van den Hoven van Genderen

geboren te ‘s-Gravenhage

promotoren: prof.mr.dr. A.R. Lodder
prof.mr.dr. A. Oskamp

Leescommissie

Prof. dr. W.G. Werner (Wouter), chair
Prof. dr. P. De Hert (Paul), Vrije Universiteit Brussel & UvT
Prof. dr. I. Lloyd (Ian), University of Southhampton, UK
Prof. dr. G.P. Mifsud Bonnici, Rijksuniversiteit Groningen
Prof. dr. T.C. Wingfield (Thomas), National defense university, Washington DC, USA

Acknowledgements

This book is the result of an extracurricular PhD research I started 7 years ago. It could not have been possible to finish this book without the help of my colleagues at Transnational Legal Studies Department, specifically my colleague and promotor Arno Lodder with his always critical remarks and advice to skip large parts of the text that was considered by him as superfluous.

Further special thanks go out to Jilian Dobson of TLS who was a great help in finding the right English grammatical construction of this book and killing incomprehensible long sentences.

Further, of course, I extend my thanks to my former colleague and promotor Anja Oskamp who could find the time to comment on my text in the time spaces during her busy task as former dean of this faculty and in her present function of rector of the Open University.

Due to the dynamics of the subject I had to adapt the text several times when new regulations were enacted and international courts as the European Court on Human Rights and the European Court of Justice issued their rulings on the relevant aspects of my thesis.

Also the publication of the 'Snowden papers' and the reactions of governments on terrorist attacks by sharpening their rules on security required changes of the text more than once. Still I had to finish my research on a certain point in time although it always was tempting to elaborate on those recent developments.

I found a great stimulus in the research for the European project on Terrorism Financing (HEMOLIA) during fouryears I functioned as Legal Executive Officer for this project. This accounted certainly for the explaining I had to do to certain partners of the project that there are privacy rules to follow, even if there should exist a terroristic threat. Not everything is allowed to reach a certain goal.

Thanks to the discussions with the international partners of the project I had even more insight in the ways of thinking by security organisations who are working in the field of anti-terrorism.

Special thanks and love go out to my partner and critical reader of my texts, Merel, who has read texts over and over during our long rides to Italy and of course for her belief in me to finish this dissertation.

Also, the many distractions of the activities of my children, Daan, Geert and Charlotte did not hinder, but stimulated the perseverance to finish this book and I really appreciate the fact that Charlotte is performing her task as paranymph next to my friend Harry.

Also special thanks to my son Geert who designed the cover of this book.

'During times of universal deceit, telling the truth becomes a revolutionary act.'

George Orwell

TABLE OF CONTENTS

1 Introduction

'The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement!'

William Pitt, English Parliamentarian, 1765

In an era where the behaviour of authorities, industry and the subjects themselves undermine the very essence of privacy, it is time to analyse the source of this behaviour from a legal perspective. We are currently living in an era of 'big data' where governments and others, like Google, collect large amounts of data about us, *nolens volens*, just for the sake of possible use in the future, crossing our thresholds without our permission.

National states have the legal and functional power to limit the fundamental rights of individuals in order to protect society for the benefit of the sum of individuals. When they do this, states are responsible for justifying their actions by grounding them in the general principles of law. In this thesis the reasoning, circumstances and legal justification underpinning these decisions will be scrutinized.

In the 21st century we witnessed two notable events, each of a completely different character, which had influential effects on the concept of privacy and the possible limitation of, and intrusion into this right by governments.

First, there was the threat of terror, embodied in the devastating attack on the World Trade Center in New York on 11 September 2001. This event prompted authorities to develop both national and international legal instruments designed to protect national security interests and combat terrorism, but at the same time intrude upon and limit the personal privacy of individuals.

The other event was the revelations by Edward Snowden, starting in 2013 about the ways, means and methods employed by national security agencies (notably the National Security Agency (NSA) of the United States and the Government Communications Headquarters (GCHQ) of the United Kingdom). The so-called Snowden files raised serious doubt and criticism of the operations of secret (intelligence) agencies.

This latter event made clear that state authorities seriously intrude on privacy, sometimes crossing the line of their legal limitations.

If we still accept that the concept of private property and virtual property, in the sense of personal information, is the source of all integrity, we have to be alert to any intrusion into privacy in the widest sense. Locke already claimed that the State's only reason for existence was its function to protect life, liberty and estate.[1] A fundamental question three hundred years

[1] Locke's (1690) main concept *Property* covers these three concepts: '(…) to preserve his Property, that is, his Life, Liberty and Estate (…).' (Second Treatise, § 87). The US Constitution is inspired by Locke, but uses another triad that includes property, viz. in the Fifth Amendment 'nor be deprived of life, liberty or property' and the Fourteenth Amendment 'nor shall any state deprive any person of life, liberty or property.' John Locke,

ago and still today pertains to how governmental authorities, in the case of fundamental rights, e.g. privacy, should balance the general interests of the State with the inviolability of the interest of the citizens whom they are obliged to protect. Fundamental rights like privacy are recognized in international treaties, e.g. the European Charter, the European Convention on Human Rights (ECHR), the International Covenant for Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR).

Fundamental to every legal system should be the following four principles as presented by the famous Dutch legal scholar Paul Scholten:[2]

1. Personality of the autonomous human being;
2. Limitations of rights only by the justice of the community;
3. Right of equality against the Authority and;
4. The separation between good and evil, the root of all justice.[3]

With regard to the concept of privacy, all of these principles are strongly connected: the right to determine what will be done with one's personal information and to what extent one's personal life is protected should be upheld above those in government; they should be applied on the basis of equality and only restricted in well-defined circumstances. Currently, however, these restrictions tend to be applied on a flexible basis.

Fundamental rights are often restricted in reaction to (perceived) threats of terrorism. The international human rights treaties do contain exceptions that allow sovereign states to restrict fundamental rights, but only if specific circumstances justify it. These circumstances are often ambiguous and are certainly not clearly defined in either national or international regulations.

The aim of this thesis is to analyse the tension between the fundamental right to privacy and the constraints under which these exceptions are justified. The specific areas studied are:

1. data protection regulations,
2. the regulations on interception and retention of personal data in the telecommunication sector,
3. money laundering and
4. the strategies used to protect national security against terrorist activities.

These areas will be commented from a predominantly European perspective.

1.1 Types of Privacy and Different Roles

Defining privacy is one of the most intractable problems in privacy studies.[4] Perhaps even more difficult is the weighing of the value of privacy against that of public interest.[5] From a socio-philosophical perspective, privacy can also be defined as a 'control-right' to which I concur:

Two Treatises of Government, (first published 1690, Penguin 1987) and: John Locke, Two Treatises of Government, Ed Thomas Hollis (London: A. Miller *et al*., 1794).

[2] Scholten 1974.

[3] Although this principle is essential, the elaboration will be consized.

[4] Reidenberg 1992.

[5] See Arendt 1949, p. 69-71, in G. Walters, 'Privacy and Security: An Ethical Analysis', *Computers and Society* 2001, p. 9.

'*A privacy right is an access control right over oneself and to information about oneself. Privacy rights also include a use or control feature—that is, privacy rights allow me exclusive use and control over personal information and specific bodies or locations.'* [6]

The fundamental right to privacy, in the sense of non-interference by government, is protected by international and national law. In its essence, the elements of privacy are based upon the non interference principle of Article 8 of the ECHR: Everyone has the right to respect for his privacy and family life, his home and his correspondence.

Although the protection of privacy, family life and communications is secured by Article 7 of the Charter of Fundamental Rights of the European Union,[7] the European Union specifies, in Article 8, the protection and control of personal data. By specifying protection and control over personal data, the Charter stresses the importance of data protection. De Hert and Gutwirth explain the differentiation between privacy and data protectionas:

> *'For us privacy is an example of a 'tool of opacity' (stopping power, setting normative limits to power), while data protection and criminal procedure can be mainly -not exclusively- seen as 'tools of transparency' (regulating and channelling necessary/reasonable/legitimate power).'*[8]

A substantial aspect of the willing or unwilling intrusion of privacy these days consists of processing of personal data of individuals, the so-called data subjects. Individuals have a strong urge to be in control of their personal information under a variety of circumstances. There is such an abundance of data, which is used in both social and commercial networks that control by the data-subject of the processing of his/her own data is almost impossible. Governments here possess and occupy two different, janus-faced roles: on the one hand, the government is the defender of privacy as a privacy regulator and authority; on the other hand, the government may legitimately 'attack' privacy, as in the Department of Justice or the Ministry of Interior Affairs. The result is as stated by the prominent scholar/theorist Westin in 'Privacy and Freedom' in 1970:

> *'Drawing the line between what is proper privacy and what becomes dangerous 'government secrecy' is a difficult task."*[9]

In criminal investigations, and certainly for the protection of national security, the use of personal data is maximized within the boundaries of the law. There is a tendency by governmental authorities to hold control over information and personal data streams. The use of personal information can then go beyond the originally-defined purpose of processing of this personal information, what can be called 'function creep.' This can result in the excessive use of personal information by authorities, insofar as it may injure the informational sovereignty of the data subject by 'function creep'.[10]

---

[6] See Adam Moore, *Defining Privacy*, Journal of Social Philosophy Volume 39, Issue 3, pages 411–428, Fall2008, p.414

[7] Charter of Fundamental Rights of the European Union (2010/C 83/02).

[8] Gutwirth, Serge and De Hert, Paul (2007). 'Privacy, Data Protection and Law Enforcement. Opacity of theIndividual and Transparency of Power.' In, Erik Claes, Antony Duff and Serge Gutwirth, eds., Privacy and the Criminal Law. Antwerpen-Oxford: Intersentia. PP. 61-104.

[9] Westin 1970, p. 49.

[10] An example in The Netherlands of 'function creep' in this respect is the extension of the use by governmental agencies concerning the electronic registration and storage of license plate registrations within the electronic number plate car registration (ANPR)'. This information can be used by police, the Ministry of Finance, Social

In this thesis, privacy is refers to the right of natural persons to control information about themselves and the non-interference by government. This definition is based on the German constitutional right of human dignity, leading to the concept of informational self-determination as created by the German Constitutional Court,'Bundesverfassungsgericht' in 1983.[11] Privacy may entail a right to a lack of disclosure of personal information but at the very least also contains a right to selective disclosure of personal information.[12] The natural person should be considered the master, sovereign over his/her privacy. The aspect of information rights to inform natural persons/subjects of processing personal information in governmental and criminal files as such will not be subject of this thesis[13].

Data protection is a separated aspect of the protection of the personal sphere on a legal basis but should be included as an aspect of privacy. This is described by Gellert and Gutwirth as follows:

'Law distinguishes between privacy and data protection. Law understands the legal right to privacy as protecting the intimacy as well as the autonomy and self-determination of citizens, whereas data protection is seen as a legal tool that regulates the processing of personal data. Ultimately, both rights are considered as instrumental tools in order to protect the political private sphere, which hallows the autonomy and determination of the individual'.[14]

1.1.1 Limitation of Privacy as a Sovereign Right of Society

Central in this thesis is Article 8 of the European Convention on Human Rights.

Article 8 of the European Convention on Human Rights provides the right for one's private and family life, home and correspondence, to be respected, subject to certain restrictions that are 'in accordance with law' and 'necessary in a democratic society. Essentially, the ECHR protects individuals from non-interference unless there are legitimate exceptions provided by the relevant authorities.

In the comments and court decisions on Article 8 of the ECHR, it is recognized that, essentially, the right to respect for one's private and family life, as well as his home and correspondence, entails that state authorities must refrain from interfering in personal privacy, whenever, wherever. Although Article 8(2) places some limits on (1), States must guarantee this right to

Security an Intelligence Agencies. In these files different governmental and non-governmental organisations will have access to sensitive personal data Different agencies, justice, tax authorities, social security and national intelligence can exchange these data amongst eachother without a transparant control mechanism. The privacy regulator has issued guidelines how to apply this competence

[11] Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, Az. : 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/8. See also: Gerrit Hornung and Christoph Schnabel, Data protection in Germany I: The population census decision and the right to informational self-determination, *Computer Law & Security Review*,Volume 25, Issue 1, 2009, Pages 84–88, citing: it would be contradicting the constitutional guarantee of human dignity for the government to claim the right to compulsorily register and index an individual's complete personality even in the anonymity provided by a statistical census, since the individual would be treated as an object accessible to an inventory in every way."

[12] McCloskey, Henry J. "Privacy and the right to privacy." *Philosophy* 55.211 (1980): p.22.

[13] I refer to transparancy of that use, in the sense of control, review, objection and erasure of personal information.

[14] Gellert and Gutwirth, *Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment*, Prescient. FP 7 project March 2013

privacy to their citizens and indeed protect it.[15] That guaranteeing in Article 8(1) should be the core of any legal instrument defining privacy or personal data protection.

Moreham in his article on the respect for private life in the European Convention on Human Rights derives even more rightss from article 8 ECHR, including:

1. the right to be free from interference with physical and psychological integrity;
2. the right to be free from unwanted access to and collection of information;
3. the right to be free from serious environmental pollution;
4. the right to be free to develop one's personality and identity;
5. and the right to be free to live one's life in a manner of one's choosing.[16]

Indentifiable aspects in the case law and commentary of the ECtHR reveals still further complementary elements falling under Article 8 of the ECHR, such as:

1. Those identifiable elements are gathered by government and business files, or
2. data gathered by security services or other organs of the state by searches and seizures, and
3. surveillance of communications and telephone conversation.[17]

The surveillance activities have been under scrutiny in the 2015 and 2016 cases by the ECtHR in the Zakharov cases[18]. Based on the last case there is a tendency to add to this list: all digital traces that reveal the whereabouts or activities of a natural person as the traffic and location data. In the end the common aspect is, they all are data considered leading to the identification of a data subject.

Privacy is increasingly challenged in case law in the face of changing socio-cultural and technological circumstances. At the same time, privacy is becoming ever more limited by governments facing unstable political circumstances and increased technological capabilities. Unsurprisingly then, it is impossible to define any absolute right to privacy unequivocally. The threat of terrorism is increasingly stimulating the intrusion of governments on personal information. After the Charlie Hebdo incident in January 2015, France passed its controversial 'surveillance Bill', giving French intelligence and police increasing its surveillance competences. After the second wave of terrorist attacks in November of that same year the determination of those inquisitive regulations is certified.

[15] Article 8(2) of the ECHR states:
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.

[16] N.A. Moreham, 'The right to respect for private life in the European Convention on Human Rights: a reexamination', 2008 *EuropeanHuman Rights Law Review* 1, no. 1, pp. 44-79.

[17] Referring to case law of the ECtHR: Weber and Saravia v. Germany and Valenzuela Contreras v. Spain,. Also *Key case-law issues. The concepts of "private and family life". Article 8 – Right to respect for private and family life,* 2007 by Antonella Galetta & Paul De Hert, Utrecht Law review, p. 57 Volume 10, Issue 1, January 2014

[18] Zakharov V. Ukraine (Application no. 26581/06)(final 07/04/2016)

It also must be kept in mind that fundamental rights are limited by the rights of other legal subjects and by regulations deemed necessary for the protection of society. The limits of the non-absolutism of privacy can be compared with the theoretical concept described by Scholten where the fundamental rights are never considered absolute. As early as 1935, Scholten stated that, although fundamental legal principles may seem undisputed, they find their limitation in other legal principles. Scholten builds further on the observation of Kant who bases his Doctrine of Right on the fact that there is only one innate right," Freedom (independence from being constrained by another's choice), insofar as it can coexist with the freedom of every other in accordance with a universal law'[19]

This relationship is always dialectic; absolutism is (according to Scholten) always relative there can be no true absolutist position because all positions are relative and that is certainly true in this era.[20]

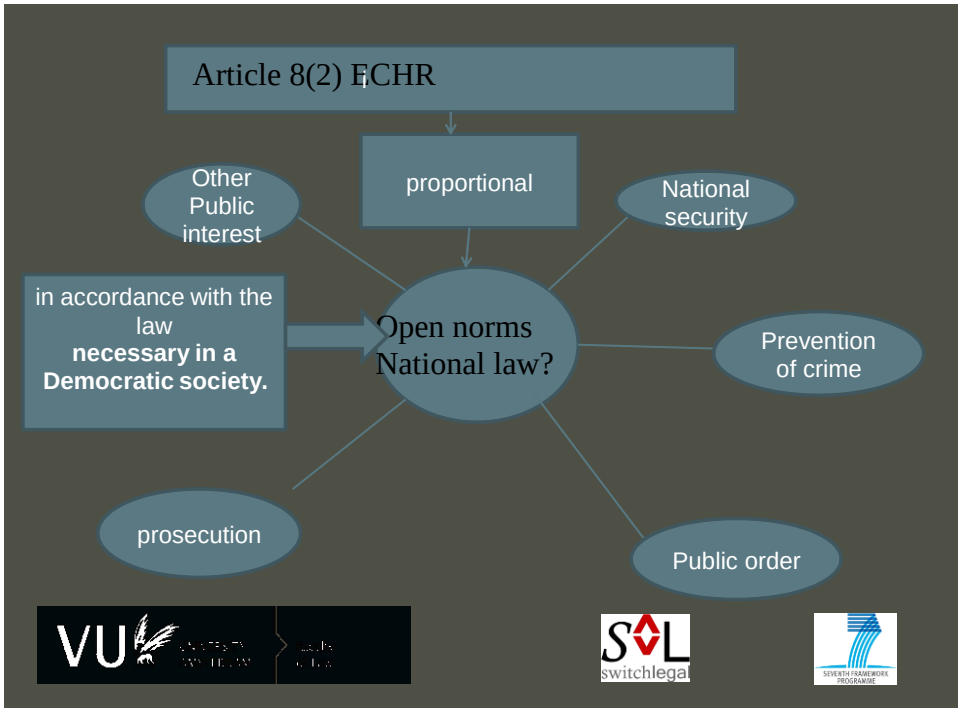
In international treaties such as the European Convention of Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR), the conflicts of rights and national policies can result in restrictions being made to fundamental rights. Article 4(1) of the ICCPR, for example, provides an opportunity to derogate from fundamental rights under the following circumstances:

'In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin'.

Limiting fundamental rights for the benefit of public goals is generally accepted in international law. The question is, under what circumstances will this opportunity to limit fundamental rights, which I would refer to as the legal 'Trojan horse', because there is always a intrusive possibility by the state to limit the given right on the seclusion of personal life and privacy.. More specifically which grounds and circumstances legitimise the State to intrude upon the citizen's rights of privacy and what procedures are in place to legitimize these intrusions? Are the international exceptions resulting in too many open norms in penal and security law?

[19] Kant, the Metaphysics of freedom, Doctrine of Public Right, 6: 314 in Immanuel Kant, practical philosophy, Camebridge University press, 12th edition 2008

[20] Scholten, 1974



Although Article 8(2) ECHR provides some grounds for limiting the rights to privacy outlined in Article 8(1), Article 15 ECHR likewise provides justifiable limits to privacy, including times of war or other public emergencies which threaten the life of the nation.[21]

Although certain threats to society, such as terrorist acts and organised crime, might be considered to form an exception under Article 15 ECHR, the threshold is much higher than the application of Article 8(2) ECHR and will be applied only when there is an imminent danger of an (terrorist) attack.[22]

In Articles 8-11 of the ECHR, concerning non-absolute fundamental rights, a number of public goals that legitimize the breach of these fundamental rights are listed. These goals include the freedoms of: the thought, conscience, religion, expression, and peaceful assembly, association with others and right to privacy.

What kind of justification may one accept to limitations to privacy, on the basis of these general principles of international law? One might defend an approach (such as that of the German Constitution) that nothing whatsoever should be done to touch the inalienable core of these fundamental rights at all. [23]

[21] Article 15 of the ECHR states that "in time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under the Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with other obligations under international law."

[22] Concerning unlawfull detention(article 5 ECHR): While it was striking that the United Kingdom had been the only Convention State to have lodged a derogation in response to the danger from al'Qaeda, the Court accepted that it had been for each Government, as the guardian of their own people's safety, to make its own assessment on the basis of the facts known to it. Weight had, therefore, to be attached to the judgment of the United Kingdom's Government and Parliament, as well as the views of the national courts, who had been better placed to assess the evidence relating to the existence of an emergency. (Grand Chamber judgment A. and Others v. the United Kingdom 19.02.09)

[23] Article 1 of the German Constitution: Human dignity shall be inviolable. To respect and protect

This idealistic approach is not practicably viable in the international nation-state system. Scholten places the rights of the individual personality in relation to those of the community to make clear that these rights have to be maintained in a different manner than the rights that have been mandated to the state community ([cf.] Rousseau). One could say that the right of personal freedom is necessary as a guarantee to support society in the functioning of those rights that have been displaced by individuals, for their preservation, to their governments.

This can result in differentiation of treatment of personal data for different purposes. For instance, is it justifiable that police data are treated in a less considerate way than 'normal' personal data? In the Dutch Act on Police Data (WPG), any data that are part of the investigation, or even data collected during police research, can be used for all kind of researches, comparisons with other cases or exchanged with other services because they are 'police data' and not protected by normal standards and principles such as those set down in the general Data Protection Act (WBP). That is acceptable if it considers the access to those data in case of a suspected person concerning severe crimes or during a critical phase of investigation if this could endanger the police work in a specific case. But is this always necessary? The national law does not distinguish these different phases and aspects of criminal investigation.

Although the subversion of fundamental rights, such as privacy, is commonplace in both national and international law, leading some to believe it is acceptable, the rules of law and politics governing such subversion are not clear.

This thesis aims to clarify what the essence of privacy is and what the limits of intrusions by government are, particularly in light of the inevitable tensions between individual rights and general interest. This contradiction should be dismantled. There should be an equilibrium between privacy as a fundamental right and the obligation of government to protect and guarantee this right, on the one hand, and the right and duty of government to limit this right under justified circumstances, based on transparent and understandable law on the other side. There needs to be a better balance established in accounting for individual rights to privacy and a general interest of safety, security and freedom. I aim to demonstrate how this equilibrium between privacy and justifiable governmental interference might be struck by unpacking the complexity of the various factors on each side.

1.1.2 Privacy as a Fundamental Right in the Information Society and the Use of Personal Information by Governmental Authorities

In the increasing complexity and interconnectness of all participants of our (information) society, the role of governmental authorities is somewhat ambivalent. Governmental authorities are responsible for ensuring protection of the fundamental rights and they have the right to intrude upon those rights for reasons of common good. States have endorsed the protection of privacy in international treaties. In this respect, based upon the commonly-held principle of the equality in the protection of privacy of legal subjects before the law, governments should have a transparent policy on the handling and use of the personal data of

It shall be the duty of all state authority. This article was applied to privacy in the sense of informational self determination in BvfG, 15 December 1983

their citizens and should be accountable for their actions. After all, non-discrimination and equality are recognised as fundamental norms of (inter)national law.[24] Next to specialized Courts as the European Court for Human Rights there is also a role for the International Court of Justice (ICJ).[25] Article 38c of the Statute of the International Court of Justice states that the general principles of law recognized by civilized nations have to be applied in its rulings. Those principles of law are also concerning the inviolability of the fundamental rights as defined in human rights treaties. But these treaties also give the opportunity to limit these right as is the case with privacy.

According to the International Court of Justice:

'the jurisdiction of a State is exclusive within the limits fixed by international law -- using this expression in its wider sense, that is to say, embracing both customary law and general as well as particular treaty law'.[26]

Therefore, inherently basic principles of human rights law have to be integrated in international and national law. But on the same level the sovereignty of the state will give opportunity to limit this right if circumstances require so. The actual application has to be specified in national law that will give too often the possibility to go beyond what has been stated on the higher level of international law.

As early as 1969, Michael Stone and Malcolm Warner warned us about the increasing power of government in the developing information age:

'The computer has given bureaucracy the gift of omniscience, if not omnipotence by putting in his hands the power to know. No fact forgotten, nothing unrecorded, nor lost, nor unforgiven'.[27]

In liberally-orientated societies there has always been, and still is, the fear of the uncontrollable powers of government. These fears were fuelled by the emergence of the 'computer', its use now commonly included in the general term 'information society'. This was actually already made clear by Orwell, as Westin puts it:

'modern societies have also brought developments that work against the achievements of privacy: density and crowding of populations; large bureaucratic organizational life; popular moods of alienation and insecurity that can lead to desires for new 'total' relations; new instruments of physical, psychological, and data surveillance (...) and the modern state, with its military, technological, and propaganda capacities to create and sustain an Orwellian control of life[28]

In Europe these fears, and more pragmatic concerns, prompted the creation of several international regulations. In particular, the treatment of personal data has been specified in

---

[24] Quotation of the Vienna Declaration and Programme of Action UN Doc. A/Conf.157/23, para. 15, by Alison Stuart, 'Back to Basics; without Distinction- a defining principle?' In: E. Brems (ed.), *Conflicts Between Fundamental Rights*, Intersentia, Antwerp-Oxford, Intersentia 2008.

[25] The International Court of Justice is the principal judicial organ of the United Nations (UN), and was established in June 1945 by the Charter of the United Nations and began work in April 1946, <http://www.icj-cij.org/court>.

[26] PCIJ, Advisory Opinion, Nationality Decrees Issued in Tunis and Morocco, Series B, Nº 4, p. 23; italics in the original text, underlining added.

[27] Stone & Warner 1969, p. 260; as quoted by Bennett 1992, p. 29.

[28] Westin 1984, p. 70.

treaties concerning the electronic processing of such data. Clear examples are the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)[29] as well as the applicable regulations by the European Union. These legal instruments are specifically directed toward the treatment of personal data, rather than privacy in its broader sense. Unsurprisingly, with the narrow focus on personal data, there is a sense of dissatisfaction in general treatment of the personal sphere within the broader perspective.[30]

The initial concentration of the Convention 108 on personal data could be broadened to the personal sphere, certainly when it considers 'the surveillance society'[31]

In the European Union the purpose of Directive 95/46/EC on Data Protection[32] is economic cooperation, but the implicit risk for privacy misuse can also be seen in the wording of this directive:

(*2)Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;*

and:

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy (...)

The so-called European Data Protection Supervisor (EDPS) recognises that the European Union is struggling with the development of the surveillance society. The EDPS cautions that measures should never go beyond what is necessary, effective and proportionate:

'Public security and combating crime and terrorism are important public objectives. However, unnecessary, disproportionate or even excessive surveillance by or on behalf of governments sows mistrust and undermines the efforts of lawmakers to address common security concerns'.[33]

[29] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981.

[30] *Aware of the major challenges and the risks posed by technological developments, and by the increasing tendency on the part of governments to carry out mass surveillance of individuals, the Conference confirms the need to modernise and strengthen the various legal frameworks for data protection, drawing on existing principles'* Resolution on the revision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Strasbourg, 5 June 2014

[31] See also: Graham Greenleaf, 'Modernising' Data Protection Convention 108*:* A Safe Basis for a Global Privacy Treaty? *(2013) Computer Law & Security Review, Vol 29, Issue 4* UNSW Law Research Paper No. 2013-33

[32] 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, *Official Journal* L 281, 23 November 1995, p. 31-50.

[33] EDPS strategy 2015-2019, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_EN.pdf

In the proposal for a General Data Protection Regulation[34], national security issues and even EU security issues are exempted from the proposed Regulation

Although a regulation has stronger harmonizing effects the chance of acceptance of such a far reaching legal instrument in this area by all European Member States is unlikely.[35]

1.1.3 Balancing Conflicting Interests and the Abundance of Information

Governments use all possible information pertaining to data subjects in order to fulfil their obligations to society in securing a peaceful and law abiding environment. From this perspective, it has been asserted that data subjects are increasingly conceived of as completely transparent both towards governments and their peers in society.[36]The possible consequences of this perceived transparency of subjects, especially with regard to the interception and retention of personal data in the telecommunications sector, has changed the strategies used to protect national security against terrorist activities.

The informational sovereignty, or informational self-determination, of data subjects is considered less important in the balancing of the values of fundamental rights and the public goals set by government. Thus state authorities are using the exceptions in cases as national security and public order or the fighting of crime, to limit or intrude on fundamental rights contained in the ECHR and the ICCPR, by stating that it is necessary for the protection of society. This can pertain a risk of function creep, crossing the borders of the granted competence, if not controlled by independent institutions.

The large quantity of personal data is a gold mine for private and public entities. The fact that they have to abide by fundamental, and less fundamental norms can however be detrimental to the pursuit of their public and private goals. Both private and public parties have specific reasons for using data, be it to enhance profit, reduce costs or make the processing of all data more efficient by using profiling techniques.

For instance, it is considered profitable for all parties that databases of medical records are made accessible to all relevant parties, such as physicians, hospitals, insurance companies and governmental health authorities. On the other hand, defending fundamental rights as the preservation of integrity of personal life and the protection of personal information as an inalienable right for individuals is also a public goal for governments.

1.2 Informational Sovereignty in a Changing World

The ‘propiska’ is a device that was used all over Eastern Europe as a residence permit, tying each person, native-born or immigrant, to a single address. Propiski were introduced by the Tsar of Russia, then Lenin banned them, Stalin reintroduced them and then the Constitutional

[34] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[35] Although considered by Koops, B.J. in *Police investigations in Internet open sources: Procedural-law issues* in: Computer Law & Security Review Volume 29, Issue 6, December 2013, Pages 654–665, par. 2.3:
The requirements are similar to those familiar from the general data protection framework although they are fine-tuned to the domain of law enforcement.

[36] Van Est, Dijstelbloem & Van ’t Hof 2008.

Court banned them again in 1991. The Mayor of Moscow announced that he intended to ignore the ban.[37]

In the era of Cyberspace,[38] a digital propiska is maintained by government, e.g. a social security (civil service) number (BSN or burgerservicenummer in The Netherlands). The digital propiska is not easily encapsulated in one particular instrument, like a social security number, but can better be conceived of as an ominous presence in all the extensions of the cyber society, usable by government but certainly not always controllable.

Certainly in the actual state of our modern 'hybrid information society', also known as the 'internet of things,' all products, applications and users are connected. Electronic chips are increasingly embedded in objects and these objects often contain internet addresses, making it very attractive for authorities and other institutions to follow and process the 'electronic traces' of their citizens:

'The European Parliament gave its backing to the development of an 'internet of things', the new information technology combining electronic chips and internet addresses, in a resolution (...).' [39]

That is agreeable as long as there is no 'state of permanent interference', i.e. a total control of all actions of natural persons by using the permanent interaction between 'things' that can be connected to an individual person (identifiability) and a (public) database that could be used by governmental institutions.[40] Hence:

'MEPs called for a proper assessment of any consequences regarding health, privacy and personal data protection. In a second resolution, parliament stressed that the internet is a global public good and should thus be run in the general interest of society'.

1.2.1 Crime and Terrorism as a R**e**ason for Interference

One observes an increasing move from 'conventional' crime to cybercrime including international terrorism, because of digitalisation, the convergence of technologies and the globalisation of ICT. Traditional investigative methods used by police and judicial authorities like surveillance and phone-tapping do not meet the demands of these changes. Lawl Enforcement Agencies (LEAs) and National Intelligence Agencies (NIAs), therefore, need special procedures to be developed and regulated, such as data mining to follow data streams, and digitalized analytical methods to assessing personal behaviour. A clear recognition of these practices by NIAs was made public in the early summer of 2013 by a former technician, turned

---

[37] D. Moss, *A submission prepared exclusively for the Home Affairs Committee in connection with its inquiry into a Surveillance Society*, Business Consultancy Services Ltd. 2007, <http://dematerialisedid.com/BCSL/HAC3.pdf>.

[38] *Cyberspace* is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. William Gibson is sometimes credited with inventing or popularizing the term by using it in his novel of 1984, *Neuromancer*. Cyberspace is often used as a metaphor for describing the non-physical terrain created by computer systems.

[39] Press release European Parliament: Information society, *Internet of Things and Governance*, June 15 2010, (Ref: 20100614IPR76044). Available at: <http://www.europarl.europa.eu/sides/getDoc.do?language=nl&type=IM PRESS&reference=20100614IPR76044>.

whistle-blower, from the National Security Agency of the United States, Edward Snowden, who disseminated information about the processing of almost all the electronic communications of certain individuals which was being done by NIAs in the Western world without proper legal justification.

The questions are, what measures can be taken by governmental and police authorities to adapt to our information society, with all its electronic information and traces? At the same time, and just as important, how can these authorities restrain themselves in such a way that preserves existing privacy rights? To what extent are authorities free to use personal data and from what sources? There is publicly available data from the internet and other public sources, but there are also data acquired in the execution of public tasks, often available in governmental databases. Are criminal investigators and security agencies allowed to use the data in the same way or in a more inquisitive way than other governmental authorities? Should data exchange by governmental agencies be allowed, and if so, under what circumstances and to what extent? Is it possible to specify laws in such a way that there is a balance between the use of the data for different purposes in the protection of privacy as a fundamental right on one hand and the protection of state integrity, as protector of the goals of national interest, on the other? Also, are the key terms and definitions used in international regulations to limit the privacy under those circumstances consistent throughout the various applications in different states?

The conviction that intelligence agencies should be allowed to perform their work in a rather uncontrolled twilight zone can be found in the Dutch government report on gathering information for intelligence agencies called *Data for Decisiveness* [Data voor Daadkracht]; citing a Dutch poet from the early 19th century:

'Although we do not know the reason why,
It probably has been done for good reason'

['Al weten wij de reden niet
't Is vast op goeden grond geschied.] [41]

Although this quotation may reflect a degree of cynicism, it clearly indicates that governments should be trusted, regardless of what they are doing with one's personal data. According to this report '*Data for Decisiveness*', the enormous growth of databases and communication media go hand in hand with the development of an advanced technological ability to search the internet which provides ample opportunity for intelligence agencies to realise their goals.[42]

In The Netherlands a bill proposing that remote computers and networks be investigated by agencies entering the networks and and which places spy-software on remote computers, to prevent computer (and other) crime, has been put forward.[43] This action would increase the investigative competence of the 'normal' investigative authorities to the level of the intelligence agencies, although to date this cannot be executed without obtaining a formal court

[41] A.C.W. Staring, *De Hoofdige Boer*, 1820. In the report of the government, *Data for Decisiveness* 2007.
[42] Reference in the report: '*The agencies are like a set of specialists in a hospital, each ordering tests, looking for symptoms, and prescribing medications. What is missing is the attending physician who makes sure they work as a team.*' The 9/11 Commission Report, p. 353.
[43] Extending article 125ja Sv Opstelten, *Minister of Justice intends to intensify investigation on internet*, Communication of the Central Government, http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/02/memorie-van-toelichting-wetsvoorstel-versterking-aanpak-computercriminaliteit.html.

order. The Netherlands NIA's though, the General Intelligence and Security Service and the Military Intelligence and Security Service (AIVD &MIVD) do not need that order for non-selective interception of any communication. A general mandate and permission of the director of the NIA or military command is sufficient.[44]

The background rationale offered by governmental authorities justifying the use of personal data is that, because of the international nature of crimes such as acts of terrorism and related crimes like money laundering, which supports these acts, international coordinated investigations and the use of personal data is needed. However, this should only be conducted whilst keeping a keen eye on the limitations necessary to safeguard the general interests of human rights and specifically to protect the privacy of individuals (taking into account the evolution of data availability).

The 'keen eye' has become rather blurred in the first decennium of the 21st century. National authorities have obtained increasing powers to limit the freedoms of individuals, e.g. on grounds of suspicion of terrorist activities. The regulations in the various European States are increasingly applied on a pro-active basis and European legislation has expanded the possibilities for judicial and investigative authorities to take measures on the basis of 'suspicious' activities.[45] One good example is the criticism on that pro-active aspect, received by the British Anti-Terrorism, Crime and Security Act 2001, which was introduced as a necessary and useful way of strengthening and defending democracy.[46] The concept of 'Lex certa', one of the basic concepts of criminal law seems to be being eroded by 'crime description creep' in the guise of protecting the democratic society.

1.2.2 Governmental Authorities are Monitoring Public and Private Information

The availability of personal data can almost be viewed as an open invitation for authorities to make use of it. Fundamental principles to limit privacy as lawfulness, proportionality and transparent purpose orientation, as stated in international treaties and integrated in national law, should not be easily set aside.

That the rights of citizens are not absolute has been discussed over the ages by renown philosophers and legal scholars as from the Middle Ages such as the famous political and legal scholar on sovereignty Bodin. There are circumstances in which certain rights may be set aside by the sovereign, as stated by Bodin in 1576[47], but this can never be in contradiction with a just interpretation of (natural) laws or the result of an unjust balancing of interests between the rights of the citizen and the 'common good' as defined by the sovereign. This is the problem we are confronted with: What is the just balance between the fundamental principle of privacy and the general interest that allows deviation from this, based on the exceptions given in

[44] Both Intelligence Agencies are regulated in the Intelligece and Security Service Act, (WIV) (Wet op de Inlichtingen en Veiligheidsdiensten, 2002, to be reformed).
[45] Senate, Justice Commission, on the law on terrorist crimes (Ek. 2003-2004, Vaste commissie v. Justitie, 28 463 Adaption of the Penal Code and other laws concerning terroristic crimes (Wijziging en aanvulling van het Wetboek van Strafrecht en enige andere wetten in verband met terroristische misdrijven (Wet terroristische misdrijven).
[46] Fenwick 2002, pp. 724-763.
[47] So the principle stands, that the prince is not subject to his own laws, or those of his predecessors, but is bound by the just and reasonable engagements which touch the interests of his subjects individually or collectively. p30 of; Six Books of the Commonwealth by Jean Bodin Abridged and translated by M. J. Tooley Basil Blackwell Oxford.

international and derived national law? Which circumstances allow state authorities to override fundamental principles? And is there a difference in the 'fundamentality' of the human rights in this perspective?

Fundamental rights to protection against torture or slavery can be deemed as (rather) absolute rights, but privacy is one of those rights that, in practice, is considered less fundamental when weighed against the upholding of the activities of the state.[48] An interesting comparison can be made with Westin's view, very appropriately expressed in 1984, when he described the surveillance state as a characterization of the modern totalitarian regime:

'The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups.[49] *Privacy is considered a kind of individualism that is considered antisocial behaviour'*

The response to this so-called antisocial behaviour by surveillance-oriented institutions and other Legal Enforcement Agencies (LEAs) and political factions is often the invocation of defensive statements such as 'why bother if you have nothing to hide?' Nevertheless, in pursuit of surveillance efforts, particularly in the face of threats of terrorism, the State must justify its incursions into individuals' right to privacy.

1.3 Method and Structure

1.3.1 Research Questions

Restrictions to fundamental rights by governments are only allowed under specific circumstances. One of these circumstances occurs when national and international threats are made against the democratic society. These threats may come from various sources, such as from alleged terrorists and computer criminals, because the information society is amorphous and is particularly vulnerable. Admittedly, there are external threats to society and the natural persons that form part of this society on the one side as we have seen in recent years. On the other side, though, the fundamental right of privacy has been under great pressure due to perceived threats to it. These external threats enhance the possibility that governmental institutions will infringe the right to privacy by adopting any number of a range of available legal or policy measures.

But where do these external threats originate? They can be of external as well as internal origin. Physical damage as well as vast damage to information infrastructure by terrorists and hackers from other states as well as from internal origin can really destabilize society. How can a society defend itself? The international legal system, as inscribed especially in treaties on human rights, contains limitations to the right to privacy and personal life. This gives

[48] Privacy can also be considered as the underestimated requirement. This is a law of nature that is not just reserved for Mankind: Animals and humans need their own space, they also share elaborate distance-setting mechanisms to define the territorial spacing of individuals in the group (except for primitive societies that have very open norms without boundaries). It seems that, without a regulated society and the authorities to guard it, there is less need to uphold fundamental rights because there is no wolf in amongst the sheep. This, however, is not possible in modern society. See Westin 1984, p. 12.
[49] Westin 1984, p. 23, citing Mead.

governmental authorities ample opportunity to limit the freedom of self-determination of one's personal information. Nevertheless, governments must continuously search for the right balance in weighing interests between individual fundamental rights and the general interests of society.

Research question:

The problem statement is that concerning the protection of national security and measures against criminal and terrorist threats, there are several rather open-ended legal provisions to intrude upon the privacy of citizens under circumstances that often are not clearly defined and often lack independent control in their execution. This leads to the question why is that the status quo?

Is it possible to create regulations that will guarantee an acceptable intrusion on privacy under specific circumstances? Are the current regulations too open-ended? Is government overstepping its competencies?

This question will be divided in the sub-questions.

In this thesis the (thin) line between governmental competency and their duty to preserve the fundamental right of informational self-determination is analysed and its merits are documented. The sub-questions of this thesis are:

1. How, how, with respect to the historical context, has the concept of privacy evolved to its present contents (Chapter 2)?
2. How does the (inter)national legal framework of human rights permit governments to limit privacy? What principles govern exceptions to privacy in this respect? (Chapter 3)
3. How does the European Court on Human Rights validate, within its case law, exceptions to privacy? On what principles are their decisions based? (Chapter 4)
4. Are electronically-based investigations, the use of personal data and other judicial coercive measures in the telecommunication field, especially the interception of communications and retention of telecommunication data, compatible with the fundamental right of data protection and privacy? (Chapter 5)
5. Are the measures initiated by international governmental organisations and non-governmental fora to control and counter terrorist and other illegitimate activities and their (financial) support, particularly considering the anti-terrorism acts, and, anti-money laundering regulation and procedures, compatible with the fundamental right of data protection and privacy? (Chapter 6)

The circumstances under which intrusions into non-absolute fundamental rights, including the right to privacy should be allowed were considered in the drafting of the Siracusa Principles in the 1980s. These principles were drafted at a conference of the United Nations Sub-Commission on Human Rights that convened in Siracusa, Sicily. The purpose of this conference was to develop a set of principles to give the limitation of human rights a legally and ethically justified basis. These principles are crucial for the consideration of the right to privacy and data protection because they help to specify the grounds for limitation of privacy. Relatedly, it will be considered whether or not the Siracusa Principles can serve as a basis for the limitation of fundamental rights in a broader sense, in the cases of public emergencies or in situations which threaten the life of a nation.

1.3.2 Structure and Research Method

This thesis is comprised of the following steps. The first step critically tests each limitation by government in the light of the rights and limitations of the relevant treaties, with reference and in comparison to other fundamental rights as defined in e.g., the UN Declarations of Human Rights and Fundamental Freedoms 1948, The European Convention on Human Rights, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), and in the UN Covenant on Civil and Political Rights.

Applicable European directives are also taken into account as well as some general regulations such as the UN principles on privacy, the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data,[50] (this latter set of guidelines has been used as a basis for the Council of Europe Data Protection Convention).[51]

The method for research comprises the study of the works of scholars in the field of legal theories on sovereignty as Bodin, Locke and Habermas, privacy, data protection experts as Westin and others in the field of terrorism, anti-money laundering and telecommunication.
Further a practical field study was part of the research by means of the research within the three year EU-project HEMOLIA as executive legal officer on anti-money laundering and financing of terrorism.[52]

1.3.3 Structure and Contents of the Chapters

In accordance with the research questions stated above, Chapter 2 discusses the meanings of personal data, privacy, limitations on public order and security from which the states of exceptions can be introduced.

These exceptions are discussed in Chapter 3 and are tested by looking into specific rules in international law and national law within Europe. To shed some light on this, the (case) law of the European Court of Justice for Human Rights is analysed. The consistency in the use of terms and definitions in data protection directives, the European Charter and the European Convention on Human Rights, is probed in Chapter 4. This enables a discussion of the possibility of applying legal limits to privacy. The rules and regulations used in telecommunications, the retention of telecommunication data for investigative purposes as well as the inconsistencies of the European Retention Directive are scrutinised and evaluated in Chapter 5.

Turning to practise, Chapter 6 considers how these rules and regulations are applied in the domains of anti-terrorism and anti-money laundering (AML) and countering the financing of terrorism (CFT) by the relevant enforcement agencies and other related authorities. Finally, The concluding Chapter 7 will elaborate which type of actions limiting the fundamental right to privacy are acceptable, in light of the international framework of protecting privacy and the application in national and international regulatory systems, based on the relevant principles of

[50] OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data 1980.
[51] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Ets No. 108], revised version: <http://bit.ly/1x3KfYy>.
[52] http://www.hemolia.eu/deliverables relevant regulations and guidelines for AML and ATF parties.

‘fair treatment’ of personal data protection (lawfulness, proportionality, use limitation, purpose specification, equality, information, etc.) as also defined in the Siracusa Principles.

The ultimate contribution of this thesis is the provision of set of circumstances under which the limitation of privacy should be allowed, including a consideration of what principles and conditions should underpin this policy.

2 The Fundamental Right of Privacy, Historical Perspective

In this chapter I provide historical and socio-legal views on the development of privacy as an important right for individuals in (modern) society. It is not an 'in-depth' study of the phenomenon, but instead discusses aspects relevant for the analysis of the limitation of privacy as perceived by Westin, on the basis of national and international regulations, which is made in the following chapters. The question addressed in this chapter is:

How, in respect of the historical context, has the concept of privacy evolved to our current understanding?

2.1 Birth Right to Privacy

'Modern' definitions of fundamental rights are largely based on the French *Déclaration des droits de l'homme et du citoyen* (1789)[53] and can also be found in the First Ten Amendments to the Constitution of the United States (1789/1791). In the famous Fourth Amendment, the first clear reference to privacy was made, inspired by an act of resistance to the illegal searches and seizures of the citizens of the 'colony' by British officers.

'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall be issued, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.' [54]

Most national constitutions adopted comparable texts. The essential element concerning privacy, or comparable fundamental rights, is the fact that the state should defer to the natural rights of its citizens.

The first privacy test case serves as a benchmark for considering the contours and limits of a right to privacy. This case concerned the marriage of the daughter of the lawyer Samuel D. Warren, who admonished publicity of intimate personal details of her marriage and her personal life,[55]

---

[53] Article 4 - La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui: ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi.
Article 10 - Nul ne doit être inquiété pour ses opinions, mêmes religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi.
Article 11 - La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi, <http://bit.ly/1giSZoS>.

[54] Interestingly enough, this right had already been identified by Sir Edward Coke, an English [jurist] and judge, in 1604 by stating that: 'The house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose.' See: A. M. F. Randolph, The Trial of Sir John Falstaff: Wherein the Fat Knight is Permitted to ..., p. 254 and A.D. Boyer, *Law, Liberty and Parliament: Selected Essays on theWritings of Sir Edward Coke*, Indianapolis: Liberty Fund 2004, <http://www.swindlelaw.com/the-history behind-the-4th-amendment/>.

[55] See the explanation in Prosser 1960, p. 423: *'All this is a most marvelous tree to grow from the wedding of the daughter of Mr. Samuel D. Warren. One is tempted to surmise that she must have been a very beautiful girl. Resembling, perhaps, that fabulous creature, the daughter of a Mr. Very, a confectioner in Regent Street, who*

'The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. (...) Modem 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'.[56]

After the devastating encroachment of human rights during World War II, the personal integrity of the human being was recognized in international treaties such as the European Convention of Human Rights (ECHR) of 1950 and the 1948 United Nations Declaration on Human Rights and Freedoms (UDHR).[57]

In a report compiled by the Human Rights Council,[58] privacy is described as:

'a fundamental right that has been defined as the 'presumption' that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others and free from state intervention and free from excessive unsolicited intervention by other uninvited individuals.'[59]

This ultimately resulted in the text of Article 12 of the Universal Declaration of Human Rights, which states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

2.2 The Background of Privacy

Privacy is the derived right of property for one's own self, the sovereignty over one's private space, home, physical and meta-physical unique integrity: freedom of body, thoughts and other manifestations of one's personal sphere. The etymology of 'privacy', from the Latin 'privatus', is interesting here because, it is two sided: deprivation from the public life and protecting the sphere of the individual.[60] This dovetails with the actual development of the governmental obligation of non-interference in matters of personal privacy. The instinct to protect one's personal sphere is explained by Westin,[61] by reference to the protection of territory, as exhibited by animals as well as by primitive tribes on an individual and group-orientated basis.

Was so wondrous fair that her presence in the shop caused three or four hundred people to assemble every day in the street before the window to look at her, so that her father was forced to send her out of town, and counsel was led to inquire whether she might not be indicted as a public nuisance This was the face that launched a thousand lawsuits. Reported in a note to Rex v. Carlisle, 6 Car. & P. 636, 172 Eng. Rep. 1397 (1834).'

[56] Warren & Brandeis 1890.

[57] In 1946 as a draft Declaration on Fundamantal Human Rights and Freedoms which, in 1948 was officially taken up as the **Universal Declaration of Human Rights (UDHR)**.

[58] M. Scheinin, '*Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism'*, United Nations 2009 A/HRC/13/37, p. 6.

[59] Cited in: Lord Lester & D. Pannick (eds.), *Human Rights Law and Practice*, London: Butterworth 2004, para. 4.82.

[60] 'Private' and 'privacy' come from the Latin *privatus*, meaning: 'withdrawn from public life, deprived of office, peculiar to oneself'.

[61] Westin 1970.

In applying these observations to Europeans, Westin identifies several key facets to his conception of privacy.

Any individual living being needs a certain area to feed himself and rest. Some creatures need more individual space than others; some need it for large groups like ants and bees, some for smaller groups like wolves, some for pairs like buzzards and storks, and some on an individual basis, like robins. Familiarly, human beings need it in all of these configurations: as members of a continent, as Europeans, as a citizen of a nation state, as a regional citizen, and even as a city inhabitant'. On a more personal level, groups and spaces are configured around families, couples and individuals. All of these groupings have their own rules and specific boundaries in terms of behaviour, privileges and privacy rules.

In search of the roots of human privacy behaviour, Westin (1984) describes and expands privacy in his classic study of the origin of modern claims to privacy. In this study, Westin refers to a comparative analysis, conducted by Murphy, of the Tuareg, a group of desert nomads who possess a dynamic desire for privacy, changing in time and place.[62] An interesting aspect in describing behaviour related to privacy is that temporal aspects are also considered relevant to the situation. Walters, a philosopher, refers to the 'privacy' scholar Westin as walking on the sociological philosophical path in 'Privacy and Freedom' in 1967 towards the explanation of privacy, is comparing the behaviour of animals with humans at any time of their development or in any culture, stating that

'*all animals seek periods of individual seclusion or small-group identity, even though our modem norms of privacy are largely absent from primitive societies where the (seclusion of) the group is considered most relevant'.* [63]

Westin compares four aspects of privacy that are culturally universal for all humans. The most straight-forward and well-known aspect of our need for privacy is the separation based on needs for the individual, the intimate family group and wider community. He explains that privacy norms vary contextually in space, culture and time. It is not uncommon for human beings to believe that they are 'watched by gods or spirits even when they are physically alone'. This feeling is acutely felt by those aware of the all-seeing eye of national authorities and of private enterprise in the tech age in which we live.

However, unlike our present-day experiences of government surveillance and encounters with handheld and wearable technology, Westin held that physical solitude in spaces like forests, beaches or churches, was crucial for personal communication with 'guardian spirits'. This solitude, or psychological privacy, can also be achieved through self-induced trances or dreams. A modern variant is the time we need to confine oneself in the attic or study and travel over the internet to escape from the physical world. Another universal element is also noted by him, namely the tendency for individuals to invade the privacy of others, driven by curiosity, which is known as gossip. Gossip sites and online harassment over the channels of Twitter and the like are rampant manifestations of this third tendency. At the same time, society guards against such anti-social conduct by employing surveillance technologies in order to protect personal and group rights, which have the undesirable effect of decreasing the feeling of control over one's privacy.

[62] Walters 2001, p. 159.

[63] Walters, a philosopher, refers to the 'privacy' scholar Westin as walking on the sociological philosophical path in 'Privacy and Freedom' in 1967 towards the explanation of privacy, comparing the behaviour of animals with humans at any time of their development or in any culture.

Although Walters asserts that 'modern' man has a greater need/desire for physical and psychological privacy, in comparison with our ancestors, and we have greater freedom to opt for privacy through socio-political means, these days of choosing privacy may be numbered. Freedom of choice as the ultimate manifestation of informational sovereignty and informational self-determination is greatly endangered by authorities' ability to control their citizens and the use and analysis of big data by the commercial information industry. Privacy, as conceived in the human rights treaties, is evidently reduced by the ultimate control by authorities in our highly surveyed society.

2.3 Philosophical Background

One may travel back as far as Aristotle as a starting point of thinking about privacy in norms and rules. Aristotle identified two distinct spheres of social life: the public sphere of politics, the *polis*, [64] and the private sphere, the *oikos*.[65] The public sphere deals with the welfare of the whole (group, country, civil society) whereas the private sphere protects concerns the individual within this public sphere. The private sphere is concerned with the protection of personal rights, whether physical or non-physical, as in one's opinions and virtues.

Informational privacy is an important aspect of personal integrity, in the sense that it allows for the protection of the individual against intrusions by the government. The philosopher Wolff asserted that all law must ubiquitously be the source of sovereignty.[66] This led him to argue that the people willingly transfer their sovereignty only when they agreed on those laws. Relatedly, Jean Bodin, the philosopher of the commonwealth, situated sovereignty within the individual. For Bodin, like Thomas Hobbes, sovereigns are situated above the law. But one must expand on this position of sovereignty because although the decision to transfer parts of this individual sovereignty lies within the individual, the sum of those transfers lie with the commonwealth, represented by a sovereign. This sovereign can be a natural person or a

---

[64] Aristotle's concept of the 'state' is interesting here: '*Let us then enumerate the functions of a state, and we shall easily elicit what we want: First, there must be food; secondly, arts, for life requires many instruments; thirdly, there must be arms, for the members of a community have need of them, and in their own hands, too, in order to maintain authority both against disobedient subjects and against external assailants; fourthly, there must be a certain amount of revenue, both for internal needs, and for the purposes of war; fifthly, or rather first, there must be a care of religion which is commonly called worship; sixthly, and most necessary of all there must be a power of deciding what is for the public interest, and what is just in men's dealings with one another. These are the services which every state may be said to need. For a state is not a mere aggregate of persons, but a union of them sufficing for the purposes of life; and if any of these things be wanting, it is as we maintain impossible that the community can be absolutely self-sufficing. A state then should be framed with a view to the fulfillment of these functions. There must be men to procure food, and artisans, and a warlike and a wealthy class, and priests, and judges to decide what is necessary and expedient.*' Politics, Book VII, nr VIII. Also: Fred Miller, Nature, Justice, and Rights in Aristotle's Politics, Published to Oxford Scholarship Online: November 2003 (*DOI: 10.1093/019823726X.001.0001*).

[65] See Newell 1987, p. 159-178. Also The Ancient Greek City-State Symposium on the occasion of the 250th Anniversary of The Royal Danish Academy of Sciences and Letters, July 1-4, 1992. Edited by Mogens Herman Hansen: '*The primary productive unit of polis society was the oikos. Within the confines of the koinonia that was the oikos, the (adult free male) citizen was master (despotes: 1260a7-1O). But to produce the material goods that sustained the oikos itself (on the micro-economic level) and the polis as a whole (on the macro-economic level) he relied upon cooperation (based on a recognition of mutual interests) as well as coercion in dealing with noncitizen oikos members (his wife, children, and slaves, if he had them)*' … <http://www.stanford.edu/group/dispersed_author/docs/PolisAristotleRawls.pdf>.

[66] Wolff 1990, p. 20.

commonwealth or republic. Although Jean Bodin claimed that sovereignty must reside in a single individual[67], both Bodin and the English philosopher Thomas Hobbes conceived the sovereign as being above the law, in its ultimate form, non-transferable. Later thinkers differed in their theories, coming to envision new loci for sovereignty.

For instance, Locke wrote his 'Two Treatises of Government' as a proponent of the humanist tradition and a believer in natural law. For him, a right of privacy is predicated on the belief that each human being has intrinsic value that is unique to him or herself and requires protection in society. One could advocate that this conviction forms the fundamental source of all human rights:

'To understand political power right, and derive it from its original, we must consider what estate all men are naturally in, and that is, a state of perfect freedom to order their actions, and dispose of their possessions and persons as they think fit, within the bounds of the law of Nature, without asking leave or depending upon the will of any other man'.[68]

The government has no sovereignty of its own – it exists to serve the people. Locke sees protection of personal liberty as the key component of a society that places its focus on the best interests of individuals and the commonwealth, because morality predates social contracts. Specifically, he claims that,

'The state of Nature has a law of Nature to govern it, which obliges every one, and reason, which is that law, teaches all mankind who will but consult it, that being all equal and independent, no one ought to harm another in his life, health, liberty or possession'.[69]

The use of personal information should be scrutinised and should not discriminate against any legal subject. It is the responsibility of the state to protect individual subjects accordingly. as a common protector of the right of nature, though, on basis of:

'*a calm reason and conscience dictate, what is proportionate to his transgression, which is so much as, may serve for reparation and restraint'.*[70]

Extending the observation of Locke, John Stuart Mill in his treatise *On Liberty*, coupled individual sovereignty and responsibility of men to the freedom to express oneself, taking into account the limits of public society and the freedom of others:

'The liberty of the individual must be thus far limited; he must not make himself a nuisance to other people. But if he refrains from molesting others in what concerns them, and merely acts according to his own inclination and judgment in things which concern himself, the same reasons which show that opinion should be free'.[71]

---

[67] Bodin's observations, concerning the vested sovereign rights of individuals towards the Prince as representative sovereign of the commonwealth, are interesting. So the principle stands, that the prince is not subject to his own laws, or those of his predecessors, but is bound by the just and reasonable engagements which touch the interests of his subjects individually or collectively. Jan Bodin, *Les six livres de la Republique*, translation by M. J. Tooley 1955, Blackwell Oxford, Chapter VIII, on sovereignty.

[68] J. Locke, *Two Treatises on Government. Book II, Chapter 2, Of the State of Nature*, Lonang 1680-1690, para. 4, <http://www.lonang.com/exlibris/locke/loc-202.htm>.

[69] Locke para. 6.

[70] Locke para. 8.

[71] Mill 1869.

Nevertheless, John Stuart Mill does not accept that a government may exceed its given rights to limit privacy, acknowledging more or less that the State community is set up for the better as a starting point, also taking Aristotle in Politeia as a point of reference:[72]

'Let us suppose, therefore, that the government is entirely at one with the people, and never thinks of exerting any power of coercion unless in agreement with what it conceives to be their voice. But I deny the right of the people to exercise such coercion, either by themselves or by their government. The power itself is illegitimate'.[73]

2.4 Modern Privacy

In a legal sense, the natural person has complete legal authority over the control of his/her personal life and personal data. No one is allowed to intrude upon this without his/her permission. This is a mutual obligation between individuals. Public legal norms will define the boundaries of these rights and the obligation to respect these boundaries.

Stepping from the philosophical background to the law, this distinction is discussed by Habermas[74] who transforms all legal and political rights into private rights (civil law), including privacy. In combination, these private rights create a common political will and policy in which every private person is represented. He explains this by stating that:

'Political rights have not only the same structure but also the same meaning as private rights that provide a space within which legal subjects are free from external compulsion. They give citizens the opportunity to assert their private interests so that, through elections, through the composition of parliamentary bodies and the selection of Government leaders, these interests finally aggregate into a political will that has an impact on the administration. In this way, citizens can, in the role of voters, supervise the exercise of governmental power so that it responds to the interests of citizens as private persons.'

Their so-called private interests cannot always be represented by the individuals themselves. They are protected by an authority that represents their interests, though one which is influenced by the individuals. Nevertheless, individuals concede a degree of their rights to the authority who, under specific circumstances, may declare a state of emergency, or comparable situations. This means that privacy is better conceived of in terms of being dynamic and adaptable to political influence.

Privacy as a fundamental right of one's personal sphere has been discussed and theorized by many scholars. The most famous concept is the one distilled by Warren and Brandeis in the Harvard Law review in 1890. It was connected to the absolute right of property, trespassing and liberty, as was understood in the historical context of the American common law system:

[72] Politeia, Book I: *'Every State is a community of some kind, and every community is established with a view to some good; for mankind always act in order to obtain that which they think good. But, if all communities aim at some good, the state or political community, which is the highest of all, and which embraces all the rest, aims at good in a greater degree than any other, and at the highest good.'*
[73] Mill 1869, Ch. 2.
[74] Habermas 1996, p. 21.

'That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. (…) Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession—intangible, as well as tangible.'[75]

What is interesting in the article of Warren and Brandeis is that they had already demonstrated an extensive vision on privacy on the basis of the ruling of Judge Cooley ten years earlier when he stated the 'right to be let alone' as the 'right of complete immunity'.[76] This vision can easily be extrapolated to the later interpretation of the dissenting opinion of judge Brandeis in the first wire-tapping case to the actual developments in a technological advanced information society:

'Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'. [77]

Thirty years later, the same author Brandeis, then acting as a judge, specified his thoughts about technological developments in an eavesdropping case,[78] and still used his comparison of the closet of thirty years before:

'But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.'

In the same case this 'terrible evolution' of limiting the personal sphere of natural persons in 'modern' society was made clear by the reference of Brandeis to the statement of Judge Rudkin:

'The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping'.[79]

---

[75] Warren & Brandeis 1890.
[76] Although Cooley was not the first to use this expression:
'*As far back as 1834, the U.S. Supreme Court mentioned that a defendant asks nothing — wants nothing, but to be let alone until it can be shown that he has violated the rights of another.' Wheaton v. Peters*, 33 U.S. 591, 634 (1834).
[77] Cooley on Torts 1888, 2d ed., p. 29.
[78] Supreme Court (Verenigde Staten) June 4, 1928, *Olmstead v. U.S.*, 277 U.S. 438, <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=277&invol=438>.
[79] Ibid 467.

The further development of these technological opportunities is under consideration in this thesis, especially the systematically increasing possibility for investigative authorities to enter the personal sphere and personal data streams of individual natural persons.

2.5 Legal Qualification of Privacy

In this thesis I refer to the fundamental right to privacy in the sense of personal informational self determination and the non-interference by government, a right which should be protected by international and national law.[80] This thesis discusses three common conceptions of privacy:

1. Privacy of personal behaviour (personal life). This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy';
2. Privacy of personal communications. Individuals may claim an interest in being able to communicate amongst themselves, using various media, without the routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'; and
3. Privacy of personal data. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy', 'personal data protection' and 'informational privacy'.[81]

Influenced by the 'tort orientation' that is common in the legal thinking within the USA, the legal scholar Prosser presents a 'tort-orientated perspective' and reviews the responsibility for privacy from the liability perspective wherein intrusions are evaluated on the basis of the damage they cause.

Prosser classifies four basic kinds of privacy rights:[82]

1. Unreasonable intrusion upon the seclusion of another, for example: physical invasion of a person's home (e.g. unwanted entry, looking into windows with binoculars or camera, tapping telephone), searching wallet or purse, repeated and persistent telephone calls, obtaining financial data (e.g. bank balance) without person's consent, etc.;
2. Appropriation of a person's name or likeness; successful assertions of this right commonly involve a defendant's use of a person's name or likeness on a product label

[80] See for other qualifications a.o.: I. Altman, *The environment and social behavior: privacy, personal space, territory, crowding,* Monterey, CA: Brooks/Cole 1975*;* H. Gross, 'The Concept of Privacy', New York University Law Review 1967, Vol. 42, No. 34; A.D. Moore, 'Defining Privacy', *Journal of Social Philosophy* 2008, Vol. 39, No. 3, p. 411-428.

[81] Also specified as seperate 'fundamental right' in the European Charter in Article 8:
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 todata which has been collected concerning him or her, and the right to have it rectified.

[82] Cooley 1888; Prosser 1971. See also: A.J. McClurg, 'Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places', *North Carolina Law Review* 1994-1995, at 989.

or in advertising a product or service. A similar concept is the 'right of publicity' in Restatement (Third) Unfair Competition §§46-47 (1995). The distinction is that privacy protects against 'injury to personal feelings', while the right of publicity protects against the unauthorized commercial exploitation of a person's name or face. As a practical matter, celebrities generally sue under the right of publicity, while ordinary citizens sue under privacy;

3. Publication of private facts, for example, income tax data, sexual relations, personal letters, family quarrels, medical treatment, photographs of person in his/her home;
4. Publication that places a person in a false light, which is similar to defamation. A successful defamation action requires that the information be false. In a privacy action the information is generally true, but the information created a false impression about the plaintiff.[83]

Only the second of these four rights is widely accepted in the USA. In addition to these four pure privacy torts, a victim might recover damages under other torts, such as intentional infliction of emotional distress, assault or trespassing.[84]

There is, of course, some criticism of the 'narrow-minded' vision of privacy from a tort perspective:

'Although Prosser certainly gave tort privacy an order and legitimacy that it had previously lacked, he also stunted its development in ways that limited its ability to adapt to the problems of the Information Age'. [85]

Although the principle of tort is widely accepted in the American legal way of thinking, one may still question the worth of a fundamental right if the damage done to it does not result in civil liability and financial retribution. In the USA, the article by Warren and Brandeis is seen as a weak lawyer's perspective and Prosser, within the clear tort-oriented American perspective, is taken to be more acceptable:

'He shaped the torts into their current form, and their strengths and weaknesses flow directly from his vision of privacy (...) Lawrence Friedman states that '[i]n hindsight, it looks as if the Warren and Brandeis idea of privacy-protection from the despicable nosiness of the media - never got much past the starting post; and is now effectively dead.' [86]

Although Richards and Solove intend to criticise the liability view advocated by Prosser, they actually assert the liability view of Prosser. Richards and Solove go further and actually have a very negative view of these revolutionaries in privacy protection, criticising Brandeis:

---

[83] This enumeration was preceded by an earlier enumeration by Prosser in 1960:
1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs ('ïntrusion');
2. Public disclosure of embarrassing private facts about the plaintiff ('public disclosure of private facts')
3. Publicity which places the plaintiff in a false light in the public eye ('false light')
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness ('appropriation').
W.L. Prosser, 'Privacy', *California Law Review* 1960, Vol. 48, pp. 383-389.

[84] See overview by R.B. Standler, <http://www.rbs2.com/privacy.htm#anchor222222>.

[85] Richards & Solove 2010.

[86] Whitman 2004; Richards and Solove 2011, p. 1891.

'Warren and Brandeis's approach to privacy was in one sense profoundly conservative, as it was part of a broader legal strategy employed by late nineteenth-century elites to protect their reputations from the masses in the face of disruptive social and technological change.'[87]

In my opinion this connotation has to be dismantled from the assumed personal, elite background which concerned the privacy and protection of the elites, in a way that enables the essence of the article of Warren and Brandeis to survive. It is about the legal and social context that is valued as such and accepted in a broader perspective than was ever recognised before.[88]

For a common understanding of privacy, it is essential to accept the core of privacy as an inalienable right of (informational) self-determination which entails the control-right over one's privacy. This right to informational privacy is essential to the defence against intrusions by third parties as well as to the right to personal control over any personal information. This includes that any personal information will be used solely within the competence of the natural person to whom this information pertains. This supports the view of Brandeis but of course, not limited to the 'elite' media aspect as suggested by Richards and Solove. The fact that intruders are liable for damage, is not always easy to translate into material damage as presented by Prosser but the liability by the third party intruder clarifies the inviolability of the right.

Amongst others, Roger Clarke[89] indicated that with the close coupling of computing and communications that have occurred, particularly since the 1980s, the challenges of privacy of personal communications and the privacy of personal data have become closely linked. The term 'information or informational privacy' refers to the combination of communications privacy and data privacy.[90]

Westin underlines the view of linking all aspects of personal information and privacy, citing Murphy, that informational privacy is a common, though not constant, factor in all social relationships. He also describes privacy as a constant process:

'Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication…'

One could add that individuals are also balancing the desire for privacy with the interests of security in the society within which s/he lives.

This process-view of Westin connects to the concept described by Bloustein in 1964, who emphasises the personal social value protected by privacy. This concept of the personal social value defines one's essence as a human being and includes individual dignity and integrity, personal autonomy and independence. Respect for these values is what grounds and unifies the

[87] Evidently following Friedman 2007.
[88] From a purely social perspective I refer to Altman; From a social point of view one could add that in society there is a dynamic concept of privacy from negative interpretation (isolation to a desired state of self-determined privacy as presented by Altman: *the concept of privacy is central to understanding environment and behaviour relationships; it provides a key link among the concepts of crowding, territorial behaviour, and personal space.* Personal space and territorial behavior function in the service of privacy needs and, as such, are *mechanisms* used to achieve desired levels of personal or group privacy. Crowding and the related topic of social isolation will be described as resulting from breakdowns in achievement of desired levels of privacy.
[89] Clarke 1996.
[90] Westin 1970, p. 12; note 28 citing Murphy 1954.

concept of privacy as encompassed by Bloustein and Westin.[91] Green criticises the position of Westin in this respect.

*'Westin defines privacy as follows: 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.' Privacy is also considered 'the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public.' This claim for privacy would seem to be as wide the mark as the cliché that privacy is 'the right to be left (*sic*) alone.' In a world of many people, many interests, and limitless activities, such a claim is far beyond the protection of law or social conventions'.*

Nevertheless, Green's criticism of Westin's overly-encompassing definition of privacy does not do justice to the difficulty of defining privacy within law and social convention. This is in part because of the dynamic nature of privacy, in terms of time, geography and culture.

The group reference is unfounded, given the individual orientation on personality rights that is stressed by Green. Green says 'the personality is a complex, closely knit, unitary organism that is vulnerable in spiritual and physical form'.[92] As a result, in his criticism, Green finds it difficult to conceive of incursions into the right to privacy in the terms of damages and liabilities which can be compensated financially. In order to be able to invoke this tort-system in the field of privacy, there must first be a clear and specific definition of the 'personality' which can be wronged and a specification of the damage.

An explanation of the encompassing tendency to the right to privacy was highlighted in the FP7 (security) European project IRISS (2012-2015), where it was noted that

'[p]rivacy is a broader concept than information privacy or data protection, and it is possible to infringe someone's privacy without processing personal data at all. […][and] the weight of the information elements has increased(…)'.[93]

According to Finn et al., writingpartners in the IRISS project, there are seven main types of privacy, including: privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy).[94] The IRISS project also considered privacy to be a vital element to Western democratic society because it is said to affect "individual self-determination; the autonomy of relationships; behavioural independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulation."[95]

---

[91] See: Bloustein 1964.
[92] Green mentions: humiliation, indignity, emotional distress, spiritual dejection, unhappiness, outrage, and even physical harm and mental disorders.
[93] IRISS project, Del. 4. p.6
[94] Finn, Wright & Friedewald 2013.
[95] To analyse privacy as a concept for what it is, or should be, the researchers also regard privacy, (at the same time) as a value, a demand and a codified right in relation to security:
'*which is broader than the right to data protection, although not separable from it, with special regard to thehistorical evolution of the concept in which the information element has become of fundamental importance in today's information society – this is especially true in the relationship between privacy and security.'*
This leads to the overall conclusion that:

Further, it is interesting to mention that the International Standardisation Organisation defined a standard for privacy principles in December 2011, (ISO 29100), that could be mentioned as functional standard to be used for general purposes by industry and government.[96] This industry standard, as ISO norms are often integrated in the law and form an influential instrument for national requirements in different sectors of the society as for implementation in privacy policy and the application of privacy enhancing technologies.

Maybe less practical but of equally general importance is the reference of the special rapporteur of the UN Commission on Human Rights to privacy as 'a fundamental human right that has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others and free from State intervention and free from excessive unsolicited intervention by other uninvited individuals.'[97]

As privacy is considered essential in several dimensions of society, governments have the obligation to defend these values in the public domain.

2.5.1 Limits to Privacy in Public Space

The notion of privacy and its interpretation has undoubtedly been influenced by the publications and case law in the United States, particularly with regard to surveillance issues. On the various conceptions of privacy, which one can have under different circumstances, there have been several clarifying cases. The often-referenced Supreme Court decision in Katz v United States[98] determined that the test of privacy was not dependent on the location of the natural person but specified a broader concept where one would have a 'reasonable expectation of privacy':

'[…] There is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable'. Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the plain view of outsiders are not protected because no intention to keep them to himself has been exhibited'.

'*privacy – similarly to security – is not a static concept, not an ideal state that one should endeavour to reach, but a dynamic concept changing throughout historical evolution and depending on the context, which has basic principles and context-dependent elements alike.'* Idem, IRISS project

[96] ISO/IEC 29100:2011 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII. (to be acquired by paying 118 CHF) See also: David Wright & Charles Raab, International Review of Law, Computers & Technology , Volume 28, Issue 3, 2014, p.281

[97] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue ,Human Rights Council Twenty-third session Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development Lester, Pannick & Helberg 2004.

[98] Supreme Court (Verenigde Staten) December 18, 1967, *Katz v. United States*, 389 U.S. 347, <https://supreme.justia.com/cases/federal/us/389/347/case.html>**;** Shattuck 1977, 16. Reference by Taylor: State Surveillance and the Right to Privacy, p. 74.

Taylor mentions subsequent cases which elaborate the notion of privacy in the 'Katz case'.In the case of 'released' information, in casu 'res derelict' or 'res nullius' items, the California v. Greenwood case is illustrative. In this case , it was ruled that citizens could have no reasonable expectation of privacy with regard to items which they discarded in the dustbin for the express purpose of having strangers take it away.[99]

'The Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home.

(a) Since respondents voluntarily left their trash for collection in an area particularly suited for public inspection, their claimed expectation of privacy in the inculpatory items they discarded was not objectively reasonable.'

Greenwood's trash was scoured by the police. One could argue that the act of putting material in a dustbin demonstrates an intention to destroy this material and therefore the search violated this intention. This is not entirely convincing when one considers that the rubbish was publicly-accessible when the former owner discarded it in such a way.

Can one reasonably assume that in open, publicly accessible spaces, such as parks or streets, people can be considered anonymous? Does it imply a degree of equality between the observer and the observed? It is sometimes difficult to discern how the actions of citizens are being observed and monitored and whether there is an equal relation between both parties. For instance, the use of cameras by public authorities and private companies, in the name of security, renders less, and sometimes a complete lack, of control over personal information.

In order to categorise these public and private spaces, Taylor refers to Feldman, who discerned several dimensions in 'privacy spheres' within society, public space, working space and home. [100] Privacy in each sphere operates in four dimensions: space, time, action and information.[101] Nowadays, with the accessibility of social media through various devices, tables, smartphones, and computers, these privacy spheres and the individuals involved are not clear-cut. Consequently, the possibility to control one's privacy is less transparent and the possibility of observation by third parties is greater.

In Friedl v. Austria, Mr. Ludwig Friedl, of Vienna, was one of the participants in a demonstration that he had organised with others to draw public attention to the plight of the homeless. Police officers, on the 17th and 19th of February 1988, photographed him, established his identity using coercion, noted his particulars and broke up the meeting on basis of Security Services Act (Sicherheitspolizeigesetz) using force to do so. This act contains provisions dealing, inter alia, with the interrogation, arrest and detention of persons, the use of direct official coercion and the gathering, use and storage of personal data, including photographs and recordings. The Constitutional Court of Austria dismissed the claim that the authorities had intruded on the privacy of Friedl. The European Commission on Human Rights, as the predecessor of the European Court of Human Rights expressed the unanimous opinion that there had been no breach of Article 8. It also took the view that there had been a breach of

[100] D. Feldman, 'Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty', *Current Legal Problems* 1994, Vol. 47, No. 2, pp. 41-71.
[101] N. Taylor, 'State Surveillance and the Right to Privacy', *Surveillance and Society* 2002, Vol. 1, No. 1, pp. 66-85, <www.surveillance-and-society.org>.

Article 13 in respect of the gathering and taking down of personal data (nineteen votes to four), but nevertheless there was no remedy in respect to the taking of photographs and their storage (fourteen votes to nine).[102] Although there was a friendly financial settlement between Friedl and the Austrian government, confirmed by the Constitutional Court, this case exemplified the difficulty of balancing various interests. This is depending on the circumstances, fitting in Feldmans's description as: privacy involves a bundle of interests, rather than a single right, so loss of part of the bundle does not entail loss of the whole'.[103]

2.6 The Limitation of Privacy in Modern Society, Including Electronic Means, Historical Leading Cases in US and Germany

It is possible to get a general measure of approaches to the new technological frontiers by briefly surveying the approaches of a few high-profile cases in the United States that have shaped the understanding of intrusion into the personal sphere.[104] Another case even expanded the right to remain silent into the domain of privacy. The case to trespass over the threshold of the private sphere,[105] referring to U.S. case law from 1893, Richmond v. Fiske where the milkman Fiske was convicted for invasion of privacy of Mrs. Richmond. As another aspect of privacy, the defendant's right of silence (so as not to incriminate himself) is considered as an element of privacy. Olmstead v United States concerned Mr. Olmstead who smuggled liquor in 1928, during the time of the Prohibition Act. The interception of his telephone lines was considered by several judges as contravening the so-called fourth and fifth amendments of the United States constitution.[106] This was the first case of an 'electronic' intrusion of privacy, specifically a case of personal communication. This concept fits within the idea of informational sovereignty or 'self-determination.' It is the individual's decision to protect his personal sphere, not to explain that (possible dark) side of his personality or even his whereabouts under the circumstances.

Sixty years later, the Federal Constitutional Court of Germany confirmed that electronic informational privacy formed a part of the earlier-accepted personal rights (*Persönlichkeitsrecht*) to freedom, which was therefore inviolable under the German Constitution.[107] This was a logical step, based on the earlier landmark deciscion by the Federal

---

[102] EComHR January 31, 1995, *Friedl v. Austria* [1995], EHRR 83, App. No. 15225/89.
[103] Feldman, 1994, p. 61.
[104] For example, Richmond v. Fiske (1893) which concerned the intrusion of the private space by passing the doorstep.and walking into the bedroom to present a milkman bill (and physically touching mrs. Richmond,also including battery by shaking her awake.

[106] The Fourth Amendment provides: 'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' And the Fifth: 'No person ... shall be compelled in any criminal case to be a witness against himself.' [277 U.S. 438, 458] It will be helpful to consider the chief cases in this court which bear upon the construction of these amendments.
[107] Federal Constitutional Court (Bundesverfassungsgericht) decision of March 3, 2004, reference number: 1 BvR 2378/98, available at <http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html> (in German): Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Art. 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1

Constitutional Court of 15. December 1983, of the right to informational self-determination as mentioned in Chapter 1. The inviolability of the home as aspect of personal life, even when it considers a crime suspect, should not be invaded lightheartedly, without proper warrants or other credible legal guarantee.

Although this inviolability was considered to be made sacred by this earlier decision [108]and eavesdropping by electronic means should normally not be allowed, there was, under certain circumstances, the possibility of using this 'acoustic surveillance' within the law.[109] Article 13(3) of the Constitution stresses though, that this technical means has to be used proportional, only to the ultimate purpose to protect society and , or national security and no other means would provide for this purpose.[110] But even then, the value of a human right might not be invaded by authorities, rationalizing that it is for the purpose of acting againsts criminality or finding the truth.[111]

Most scholars refer instead to the positive orientation without its limitation, as referred to by Green on the American Bill of Rights: '(that) gives the individual constitutional protection of important aspects of his privacy against their invasion by state and federal officials'.

So the positive aspect is considered to be the protection of the personal sphere around the individual, be it by measures, policy or by any rule in the legal framework. This includes any physical or non-physical 'personality space'. Green states that

'[t]he individual's seclusion in his home, office, hotel, hospital room, or other place of withdrawal is protected against intrusion except by his consent or under authority of law. He is protected from physical intrusion by another person, and also from intrusion by camera, microphone, wiretap, or other electronic device.'[112]

---

i.V.m. Art. 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt. BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. (1- 373), Available at: <http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html>.

[108] Article 10 of the German Constitution states: '(1) Privacy of letters, posts and telecommunications shall be inviolable. 2) Restrictions may only be ordered pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

[109] Nicht jede akustische Überwachung von Wohnraum verletzt den Menschenwürdegehalt des Art. 13 Abs. 1 GG. BVerfG, 1 BvR 2378/98 vom 3.3.2004, Absatz-Nr. (1 - 373), <http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html>.

[110] **(3)** If particular facts justify the suspicion that any person hascommitted an especially serious crime specifically defined by a law, technical means of acoustical surveillance of any home in which the suspect is supposedly staying may be employed pursuant to judicial order for the purpose of prosecuting the offence, provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive. The authorisation shall be for a limitedtime. The order shall be issued by a panel composed of three judges. When time is of the essence, it may also beissued by a single judge..

[111] Die Menschenwürde wird nicht schon dadurch verletzt, dass jemand zum Adressaten von Maßnahmen der Strafverfolgung wird, wohl aber dann, wenn durch die Art der ergriffenen Maßnahme die Subjektqualität des Betroffenen grundsätzlich in Frage gestellt wird. Das ist der Fall, wenn die Behandlung durch die öffentliche Gewalt die Achtung des Wertes vermissen lässt, der jedem Menschen um seiner selbst willen zukommt. Solche \ Maßnahmen dürfen auch nicht im Interesse der Effektivität der Strafrechtspflege und der Wahrheitserforschung vorgenommen werden.. Federal Constitutional Court (Bundesverfassungsgericht) decision of March 3, 2004, par. 117

[112] Green, p.752

Green mentions that this must also have been 'doubtless' in the minds of Warren and Brandeis when they wrote their article.

It was likewise 'doubtless' in the mind of Green to extend this conception to the electronic seclusion of the personal mail, electronic mail and internet traces, commercial and public databases and GPS traces. He further extends his privacy concept to photos made in public spaces of persons in very specific circumstances that would invade the person's personal sphere, sharing the original point of departure taken by Warren and Brandeis.

Governments have developed a high level of surveillance by using all sorts of data and all kinds of inquisitive methods to exercise their given task of protecting the rights of all citizens and maintaining equilibrium in society. The instruments that are used to do this are continuously piercing the privacy of their citizens. To control societal processes, information is gathered by the use of cameras on street corners, drones, remote sensing satellites and are processed to filter relevant information about citizens.

2.7 Right of Intrusion as a Negative Aspect of Privacy

Although the term 'negative right' usually refers to the aspect of the non-intrusion of governments on fundamental rights, this negative right actually takes the form of the intrusion itself. This right of intrusion, as found in Article 8(2) ECHR, and comparable law, can be considered as the negative right to limit and intrude upon those rights.

One may consider the aspect to be in the public sphere as well as in the private one:

'A person may be asserting his right of 'privacy' when he dresses in in an unorthodox way or when he 'loafs' in a public park. A person may claim the right to be let alone when he acts publicly as when he acts privately. Its essence is the claim that there is a sphere of space that has not been dedicated to public use or control.'[113]

With the increased application of technological means to public spaces and communication infrastructures, the credible existence of the state is endangered.[114] The credibility of the state as the defender and caretaker of the fundamental right to privacy will, at the very least, be corroded.

Returning to Westin, the proportions of the task which he has undertaken, defining privacy, become painfully clear when one considers the nature of the subject he is seeking to analyse. Brandeis defined privacy as 'the right to be let alone,'[115] suggesting the absence of any identifiable boundaries to the concept. In his conceptualisation of privacy, Westin brings us back to the four 'states of privacy' that he distinguished - solitude, intimacy, anonymity and reserve.

Limitations imposed on these rights, on the basis of promoting the general interests of society, for instance maintaining national security, protecting the public order or preventing crime,

[113] Konvitz 1966.
[114] See also: Ch. Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment,* University of Chicago Press 2007, p. xi and further.
[115] Supreme Court (United States) June 4, 1928, *Olmstead v. U.S.*, 277 U.S. 438.

intrude on the solitude, intimacy and anonymity of the individual and on his right to reserve control over his information.

Within the duality of Westin's privacy concept, in terms of the determination of one's communication of information and the 'withdrawal' from civil society, society is inclined to accept that the limitations are exercised by the authorities in good faith by trusting in, or acquiescence to, a belief that the limits of the powers of the authorities will not be misused. This attitude can be explained by Westin's concept of one of the primitive aspects of privacy: the reference to the will of gods or spirits and the belief that authorities know what is best for the people. This belief mixes reverence, resignation and fear and results in people proffering the familiar reason for giving up control over privacy and personal information to the authorities:

If you have nothing to hide why bother?

But if we accept that privacy concerns the whole sphere of control by the individual over his personal integrity, information and communication, including his whereabouts, then one should bother. The idea that the individual cannot control which information about him is used by other parties will result in a disconcerting feeling.[116]

The juxtaposition is, in fact, the idea that everyone should be the master of his own personal sphere but cannot truly be. The fact that there is a personal right of self-determination also gives the opportunity to mandate authorities to use the personal information and limit the protection of privacy if circumstances require it. The societal mandate given to parliament and governmental authorities provides an opportunity for limiting the privacy based on law and national policy.

The conclusion is that privacy is the area surrounding a natural person's personal life, which is not to be invaded by the government (or other third parties) unless explicit or implied permission is given by the natural person himself.

Implied permission, as current practise reveals, includes an extensive interpretation of security laws and (formal) criminal laws. The obvious problem is one of limits and the extension of the function creep and competence creep, whose boundaries are hard to define. This fear was raised in a report by the Committee on Civil Liberties which was composed by the Justice and Home Affairs of the European Parliament (Libe) and the Commission of the European Parliament, which states:

'Right to privacy, respect of the integrity and the dignity of the individual are at stake. Mass collections of data with no respect for EU data protection rules and specific violations of the proportionality principle in the data management run counter to the constitutional traditions of the Member States and the fundaments of the European constitutional order'. [117]

It is interesting to see that, within the European Union context, there is a shift from the original protection of personal data within the context of supporting a European service industry

[116] *The objective category of privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information* Calo, 2011, p. 1131

[117] European Parliament, *Committee on Civil Liberties, Justice and Home Affairs* 2009-2014, p. 39.

without borders, by harmonizing the data protection system, to a more privacy-orientated protection of fundamental values.

2.8 Privacy and Data Protection in the European Union

2.8.1 Privacy in the TEU and the TFEU

In Article 2 of the TFEU, a declaration of general respect for fundamental rights, respect for the law and the equality principle is made. The aspects of freedom, justice and security for all EU citizens are within the competence of the Union and will be applied according to the principles of subsidiarity and proportionality. In Article 4 of the TFEU, freedom, security and justice belong to the shared competences of the EU and the Union and Member States have the competence to create legislation in that field. But the Member States can exercise their competence only to the extent that the Union has not exercised its powers.

Combined with the fact that the EU will adhere to all the international principles of the United Nations Charter, a direct reference is made to the normative character of the legal framework of the European Union by Ian Manners in his article on the Lisbon Treaty (reform treaty). Manners characterises the principles and values, which are derived from other constitutive documents, such as the UN Charter and the European Convention on Human rights, as a the product of a process of constitutionalisation. According to Manners, this occurred between 1995 and 2012 and consolidated a trinity of democracy, human rights and the rule of law as the keystone of European internal and external action. In addition, the EU principle of cosmopolitan law advances the development and participation of the EU and its member states in humanitarian law and rights applicable to individuals; significant emphasis has been placed on the promotion of good governance through the participation of civil society in order to encourage openness and transparency, as well as to facilitate democratic participation. This is only possible when there is a harmonized and consistent policy on privacy and security[118].

Still we have to take in account that the tendency to a more dualistic approach of the ECJ towards legal instruments of non EU international organisations could result in a too simple conclusion. In the so called Kadi cases, the ECJ reviewed the lawfulness of the EU regulation transposing a resolution of the Security Council of the UN for sanctions against Al Quaida.[119] The transposed EU regulation resulted in a freeze of the assets of Kadi in Europe. Kadi contested this. The ECJ concluded that the protection of fundamental rights forms part of the very foundations of the Union legal order and therefore all Union measures must be compatible with fundamental rights. The SC resolution (and the EU regulation) had not guaranteed those rights. Kadi had not been informed of the grounds for his placement on the list of individuals and entities subject to the sanctions. Therefore he had no possibility for hearing judicial review. But this should be based on European Law because the EU has his own legal order as was long before decided in the van Gend & Loos cases.[120]

---

[119] Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v. Council and Commission.* Also referred to in chapter 3 and 5.
[2008] ECR I–6351.
[120] For more extensive description of these cases see:

Consistency means ensuring that the EU is not hypocritical in promoting norms which it does not itself comply with.[121] As Kalypso Nicolaidis and Dimitri Nicolaidis have put it:

'Fundamentally, normative power can only be applied credibly under a key condition: consistency between internal policies and external prescriptions and actions.'[122]

This consistency can be achieved by, amongst other things, integrating important fundamental legal instruments in the European legal framework. Integrating the Charter of the EU into the EU legal framework is a step in the right direction. The relevance of this human rights oriented policy is i.e. made clear by deciscions in the annulment of the retention directive and the annulment of the 'Save Harbour Agreement' in the 'Schrems case" as is amply discussed in Chapter five and seven.[123]

2.8.2 Charter of Fundamental Rights of the European Union (2000/C 364/01)

The much discussed EU Charter of Fundamental Rights forms the core of the protection of the personal sphere within the European community. Although considered legally binding, as stated in Article 6 of the TEU, the legal structure is unlike a treaty.

Nevertheless, it has the same binding character and is considered to be of the same legal value as the treaties.

It is strongly based upon the European Convention on Human Rights and one can see a continuing development of the integration between the fundamental rights of the ECHR and the EU in the legal instruments. This Charter, with due regard for the powers and tasks of the Community and the Union and the principle of subsidiarity, reaffirms the rights as they result, in particular, from the constitutional traditions and international obligations common to the member states. This includes the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Community and by the Council of Europe and the case-law of the Court of Justice of the European Communities and the European Court of Human Rights.

The Charter encompasses, in the broadest sense, a concept of privacy through Articles 1-8 and in Article 11. However, EU law provides room for exceptions under Article 52, based upon the principle of proportionality and deemed necessary to meet the objectives of the Union and the need to protect the rights and freedoms of its citizens.

Juliane Kokott and Christoph Sobotta: *The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?,* The European Journal of International Law Vol. 23 no. 4, 2012

[121] I. Manners, p. 76 note 42, Kalypso Nicolaidis and Dimitri Nicolaidis, 'The EuroMed beyond civilisationalparadigms', in Emanuel Adler, Federica Bicchi, Beverly Crawford and Raffaella Del Sarto, eds, *The convergence of civilisations: constructing a Mediterranean region*, Toronto: University of Toronto Press 2006, pp. 348-349.

[123] Case C-362/14 , 16 October 2015 *Maximillian Schrems v Data Protection Commissioner* [2015]
Cases C-293/12 and C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland Ltd v. Minister for Communications* [2012].

The necessity of adhering to the Charter and the principles of the ECHR is stressed in the so-called Declaration of Stockholm.[124] The paragraph in the declaration that stresses the inconsistency of the relevant definitions in different legal instruments and their inconsistency among the different European Member States is particularly relevant:

'the principle of availability is liable to allow the exchange of personal data that have not been collected legitimately and lawfully, and that it must be underpinned by common rules; expresses doubts with regard to the facilitation of operational activities that do not include a European definition and common standards concerning covert investigations, surveillance of citizens, etc.'

According to the interpretation of Article 16 of the TFEU, this requires the legislator to lay down rules relating to the protection of individuals with regard to the processing of personal data, also in the areas of judicial co-operation in criminal matters and police cooperation, covering both cross-border and domestic processing of personal data. This will allow the fundamental rights and freedoms of natural persons to be protected and, in particular, their right to the protection of personal data, whilst simultaneously ensuring that the exchange of personal data, for the purposes of prevention, investigation, detection or prosecution of criminal activities, is safeguarded.

This interpretation is stressed again in the mid-term review of the Stockholm program:

'1. Believes that the Treaty of Lisbon and the recognition of the legally binding force of the Charter of Fundamental Rights of the European Union have brought significant improvements and strengthened the constitutional basis for the EU institutions and the Member States to achieve the objective of establishing an area of freedom, security and justice, but observes that some areas require additional efforts, in particular as regards their implementation; considers that this objective requires the Treaties and secondary law to be applied evenly throughout the EU; agrees, therefore, that opt-outs or special regimes should be avoided, and where possible removed.'[125]

In this review two types of warnings are issued. The first is to adhere to the legally binding Charter and the second, directed to the European institutions and the individual member states warns against limiting fundamental rights light-heartedly.

The ECJ already has applied the Charter in several cases by ruling that inconsistencies with the Charter are against the European legal order.[126] National legislation implementing EU law should be set aside if it conflicts with the rights contained in the Charter.[127] And even EU directives can be annulled by the ECJ if contrary to the Charter as will be extensively be explained later in this thesis.[128]

---

[124] European Parliament resolution of November 25, 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2009-0090&language=EN>.

[125] L. Berlinguer, J.F. López Aguilar & C. Casini, *Report on the mid-term review of the Stockholm Programme* 2014.

[126] Joined Cases C-92/09 and C-93/09 *Schecke*

[127] C-396/11 *Radu* and C-399/11 *Melloni* cases

[128] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*

The EU is also trying to become a full party to the ECHR as such. The proposed agreement of the EU for accession to the ECHR though, was considered incompatible with the provisions of the EU law as of the 18th of December 2014.[129] The European Commission will have to go back to the negotiating table.

2.8.3 Data Protection in the European Union: Constraints and Opportunities

The Charter differentiates between privacy and personal data protection. The current legal instrument within Europe that regulates the existing personal data protection is Directive 95/46 which is based on two fundamental aspects:

1. The enhancement of the internal market and
2. The protection of personal data in the (international) processing of data.

As stated in Recital 3 of Directive 95/46:

'Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.'

This Directive gives ample opportunity for differences of interpretation within the Member States. As made clear by Recital 22 TEU:

'Whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8.'

Even the processing of data and, more specifically, the access to it, may be available to an undefined number of parties, as explained in Recital 30 TEU:

'or for the performance of a task carried out in the public interest or in the exercise of official authority'.

Perhaps most significantly, there is plenty of opportunity to define individual legislation for the use of data in security matters, as is made clear by the reference made in Article 4.2 TEU:

'In particular, national security remains the sole responsibility of each Member State.'

The result is a divergent system of national rules that regulate personal data protection, especially the limitations of its use in criminal law efforts and in national security concerns. The European Commission also remarked on the incoherence when evaluating the application of the Directive in national legal systems, stating,

'Under the current Data Protection Directive 95/46/EC, a company operating in more than one EU country will have to deal with several Data Protection Authorities ('DPAs') with very different powers (up to one per member state). This leads to uncertainty for business and to

[129] http://bit.ly/19PkPrp

situations in which different rules can apply in each member state for the same operation. There is no system for reconciling different DPA decisions apart from having non-binding discussion of the sort described in the so-called Article 29 Working Party, which brings together EU DPAs'.[130]

With regard to the harmonization of definitions of criminal offences in criminal law, a.m. anti-money laundering and anti-terrorism financing, which can provide authorities with an opportunity to limit the protective provisions in privacy law, only a rather weak minimum line is given in Article 83 TFEU:

1. The European Parliament and the Council may, (...) establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.

The ultimate escape though is provided by the powerlessness of European judicial competence which is described in Article 276 TFEU:

in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

The aforementioned provisions give ample opportunity for broad divergence among the member states and will create insecurity for Law Enforcement Agencies as well as for the subjects of investigations if the European Court of Justice does not assume jurisdiction over the European-initiated regulations and directives in this area although there are several legal instruments within European competences on specific areas, within law enforcement a general harmonisation is not present.[131] In the European Council decisision a police cooperation has been constructed to simplify police assistance and cooperation between the Member States, this does not harmonize the protection of personal data.[132] Also within the Schengen Agreement a derogation from the protection of personal data is possible, based on national regulations.[133] This could also disturb the use of harmonized procedures because descriptions of the offences are different, and it may foster opportunism, exploiting opportunities as companies and individuals search for options in particular countries that are not allowed in other countries. It is doubtful if the ECJ will rule on such sensitive issues in law enforcement matters. This

[130] http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm

[131] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

[132] COUNCIL DECISION of 6 April 2009 establishing the European Police Office (Europol)

[133] Article 102.3: any derogation from paragraph 1 in order to change from one category of alert to another must be justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence.

expectation is supported by the fact that the proposed directive on protection of personal data in criminal justice of the legal framework makes an exemption for these organisation, although a precedent is set in the annulment ruling of the retention directive. This also would apply to the discussions on PNR (Passenger Name Record) and TFTP (Terrorist Financing Tracking Programme) agreements.

This problem can be solved by defining the offences clearly in the more specific criminal law and privacy law branches, which can then be tested by national courts and the ECtHR. The question is: will this be made possible by a future legal framework? This will be addressed in the next section.

2.8.4 Proposal for a New Legal Framework for the Protection of Privacy and the Free Movement of Personal Data (General Data Protection Regulation, GDPR)[134]

On the 25 January 2012, a 'new' regulatory framework on the protection of privacy and personal data in the EU, was presented by the European Commission as set out in Communication COM (2012) 9 final. The proposed new legal framework consists of two legislative proposals:

1. A proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), and
2. A proposal for a Directive of the European Parliament and of the Council 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.[135]

The General Data Protection Regulation is according to the Commission intended to:

'[i]mprove the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities.'

The current proposal is to strengthen the protection of personal data by taking functional and technological measures and define more clearly when exceptions to the rights of data protection for data subjects are possible. Clearly there are challenges inherent to the drawing of these limits, particularly when concerning the governmental use of personal data.

'At the same time, ways of collecting personal data have become increasingly elaborated and less easily detectable (…). And the growing use of procedures allowing automatic data collection, such as electronic transport ticketing, road toll collecting or of geo-location devices make it easier to determine the location of individuals simply because they use a mobile device. Public authorities also use more and more personal data for various purposes, such as tracing

[134] COM (2012) 11 final. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation). January 25, 2012 COM (2012) 11 final 2012/0011 (COD).
[135] COM (2012) 10 final.

individuals in the event of an outbreak of a communicable disease, for preventing and fighting terrorism and crime more'.[136]

The actual responsibility of the Member States as authorities has not been indicated but consultation among Member States has created a transnational result, enabling a (new) legal basis (Article 16 TFEU) to be created which allows the EU to have a single legal instrument for regulating data protection. In the proposed action, the areas of police and judicial cooperation in criminal matters are also indicated, meaning that the area of Common Foreign and Security Policy is only partly covered by Article 16 TFEU. This is because specific rules for data processing by member states must be laid down by a Council Decision which has a different legal basis. This common position is exemplified in the proposals that were published in January 2012.

As a result of the evaluation of the existing framework, it was stressed that the current fragmentation of personal data protection in the European Union was the main problem, in particular by economic stakeholders who asked for increased legal certainty and harmonization of the rules on the protection of personal data. The other point that was stressed was the complexity of the rules on international transfers of personal data. This is considered as a substantial impediment to the stakeholders operations as they regularly need to transfer personal data from the EU to other parts of the world.

This new regulatory proposal was chosen in order to create a sturdier legal instrument that could fend off the criticism that privacy protection within Europe was a low-quality patchwork blanket. As stated in the memorandum of the proposal, the purpose was to create better protection for the three policy objectives, namely: to improve the internal market dimension of data protection, to make the exercise of data protection rights by individuals more effective and, to create a comprehensive and coherent framework covering all areas of Union competence, including police co-operation and judicial co-operation in criminal matters.

Therefore the legal instrument of a regulation was chosen by the Commission to regulate data protection and data transfer within the European Union.

Although opting for a regulation with its direct applicability (Article 288 TFEU) is understandable, choosing the most inflexible, far-stretching legal instrument of the Union will certainly create problems as well. Of course, the use of a regulation reduces legal fragmentation and provides for a greater legal certainty by introducing a harmonised set of core rules and therefore will be

'Improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market'.

But a stringent harmonization of already existing divergent national privacy regulations and policies in 28 member states will represent a strong challenge to sovereignty, based on the subsidiarity principle. On the positive side, the use of a regulation promises to underline the importance of the protection of the personal life of the European citizen.

[136] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions A comprehensive approach on personal data protection in the European Union /* COM/2010/0609 final */, p.2

But, of course, and again, limiting the practical implementation of the right to privacy and the protection of the personal life is still the prerogative of national authorities on the common ground of public safety and security.

It would have been wise to strengthen the competence of a supervisory authority regarding the interpretative boundaries of this freedom of the member states, as they do not have the powers of the Commission or another (independent) institution which could be used as a safety valve.

The question is whether the determination of the non-applicability of the principles of the data protection regulation in security matters would also be an issue that could be handled by this authority. There is also the matter of consistency in the application of principles in the regulation as these seem to be directed more towards harmonising procedures than to regulating and applying the content.

Consistency is addressed in Article 59, wherein the Commission may either reinforce the opinion of the European Data Protection Board or express a divergence with that opinion. It also contains measures of the supervisory authority. Where the matter has been raised by the European Data Protection Board under Article 58(3), it can be expected that the Commission will exercise its discretion and deliver an opinion whenever necessary.

Strangely enough, mutual assistance seems to apply to the cooperation and not to the protection of personal data protection principles. Article 55 introduces explicit rules on mandatory mutual assistance, including the consequences for non-compliance with the request of another supervisory authority. Article 56 introduces rules on joint operations, inspired by Article 17 of Council Decision 2008/615/JHA, including a right of supervisory authorities to participate in such operations. The contents of this initiative is made clear in the subsequent decision where restraint based on privacy considerations seems to disappear in the thinking of the European Union especially when security issues are at stake, like combatting terrorism, cross-border crime and illegal migration. Article 5 of the Council decision is very clear here, stating:

'Member States shall take all necessary measures to ensure that automated searching or comparison of DNA data, dactyloscopic data and vehicle registration data is possible 24 hours a day and seven days a week.'

Although the GDPR requires active participation, under Article 55, in the exchange of personal data between supervisory authorities, the application of the Regulation as such, including the protective purposes of the directive are exempted in consideration 16 of the Regulation.[137]

2.8.5 Directive on the Protection of Personal Data by the Processing of Such Data by

[137] Consideration 16 states that the protection of individuals with regard to the processing of personal data bycompetent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, ***or the safeguarding against and the prevention ofthreats to public security*** and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by themore specific legal instrument at Union level (Directive XX/YYY).(note: in the 2015 Council version this consideration is even more extended to give member state opportunities to specify the application of the regulation, moving towards the formal scope of a directive!)

Criminal Justice Authorities (Justice Data Directive, JDD)[138]

Data that is processed by public authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is governed by the directive in the title of this section. This directive strives to "strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations."[139]

Personal data may be used if it is deemed necessary for the performance of a task carried out by a competent authority based on national law. The use of personal data must comply with the legal obligation to which the data controller is subject, in order (to protect the vital interests of the data subject or another person) or to prevent an immediate and serious threat to public security.

The objective of the proposed Directive is to combat the flaws of the Framework Decision 2008/977/JHA which has a limited scope of application, as it only applies to cross-border data processing and not to processing activities conducted by the police and judiciary authorities at the national level. The criticisms of the Framework Decision concern the fact that authorities do not always seem to be able to easily distinguish between purely domestic and cross-border processing, or to foresee whether certain personal data could become the object of a cross-border exchange at a later stage. Moreover, because of its nature and content, the Framework Decision leaves room for Member States to manoeuvre when implementing its provisions in national laws. Additionally, it does not contain any mechanism or advisory group, similar to the Article 29 Working Party, to support common interpretation of its provisions, nor does it foresee any implementing powers for the Commission to ensure a common approach in its implementation.

The Directive cannot reach the same level of privacy protection as the proposed Data Protection Regulation. In that regard the European Data Protection Supervisor (EDPS) stated, inter alia, that

'The widening of the scope of application only has added value if the Directive substantially increases the level of data protection in this area, which is not the case. Compared to the proposed Regulation, many provisions in the proposed Directive are weak, without any evident justification.'[140]

The declared goal of the reform is not fully achieved and the lack of comprehensiveness has not been remedied.The directive still gives opportunity for lack ofharmonisation amongst the Member staes and has too many open terms that can create legal uncertainty.

In the following section, the limits of this Directive will be considered by comparing various sections in which the limitation is stated. Further a list of terms will be analysed to identify how the contents of these definitions are the same or comparable or are so different that this

[138] For this chapter the Council text of 29 June 2015, nr. 97 was used

[139] Proposal for a directive of the European Parliament and of the Council 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 {SEC(2012) 72 final}.

[140] EDPS Opinion on the Data Protection Reform Package of January 2012, pt. 19.

could have a negative influence on the protection of the privacy of the subjects this protection concerns.

2.8.6 Differentiation of Data Subjects in the Proposed Directive

A positive development in the proposed Directive is an evolution of the concept of the data subject. The differentiation within different kinds of data subjects has not been present in any of the preceding European legal instruments on this subject. The differentiation between 'real suspects' and 'connected third parties' is considered to result in different treatment of the protection of the personal data among different categories of data subjects.

Although the original text of Article 5 is quite an improvement in comparison to the existing regulations and national laws under which there was no distinction of data subjects, there is no indication of the consequences of this distinction, nor is there any indication as to how the controller should apply these distinctions. In the Council text, the title of the Article 5 is the only aspect that remains. The content is removed and only Austria is in favour of a revival of the content.[141]

Paragraph 4 of the JDD, which concerns the obligation to process personal data lawfully and fairly, is particularly interesting because it outlines limits but extends wide-ranging permissions. Unsurprisingly, data must be collected for specified, explicit and legitimate purposes and may only be processed in a way compatible with those purposes, adequate, relevant, and not excessive in relation to the purposes for which they are processed, and, where necessary kept up to date for no longer than is necessary for the purposes for which the personal data are processed. However, futher processing, by the same controller for another purpose, shall1 be permitted as long as: it is compatible with the purposes for which the personal data was collected; the controller is authorised to process personal data for such purpose in accordance with the applicable legal provisions; and the processing is necessary and proportionate to that other purpose.

Further all information rights for the subject are provided for in Articles 10 and 11 but Article 11(b) provides some important limitations. These include the adoption of legislative measures delaying, restricting or omitting the provision of the information to the data:
to avoid obstructing official or legal inquiries, investigations or procedures or to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; and of course to protect public and national security.

This could open possibilities for legally based withdrawal of the guarantees in case of endangering, criminal investigations and national and public security. In March 2013 the Article 29 Working Party stressed that this Directive was not a very serious investment in making a comprehensive data protection instrument. The WP rates this Directive as a disappointment in its lack of ambition compared to the GDPR. It is interesting that even for the former so-called third pillar activities, the WP believes that the same high-level of data protection should ultimately be applicable to all data processing in this area, including by the EU bodies.

[141] Council text of 29 June 2015, p.54

Additionally, the WP 29 finds fault in the grey area of personal data exchange between national authorities and more-or-less private parties is a subject of concern because strict conditions for data transfers between law enforcement authorities and other (semi)public and private parties are not in place or unclear.

Nevertheless, the European Commission remains optimistic that this Directive may lead to considerable improvements that harmonise data protection enforcement and give individuals the ability to exercise their rights to data protection within the EU.

At the time of concluding this text the Regulation and Directive are still in the dynamic phase of negotiating on the definitive version.

2.9 Concluding Remarks on the Development of Privacy

The question addressed in this chapter was:

How, with respect to the historical context, has the concept of privacy evolved to its present contents?

The concept of privacy has developed into a dynamic non-absolute right that is constantly in flux, shaped by the social and political contexts of society. The essential element concerning privacy, and comparable fundamental rights, is the fact that the state should defer to the natural rights of its citizens; the duty of the state is not to interfere with these natural rights.

The role of government is nevertheless ambiguous. It has to defend privacy as fundamental right on the one hand, but may also, in the name of protecting this fundamental right and the public order and national security, limit privacy as required. The growing complexity of society and technological developments demands for a continuously growing balancing act in this respect.

The philosophical overview provided a few basic principles entailed in the right to privacy. As Locke stated, the government has no sovereignty of its own - it exists to serve the people. The key component of a society is, that it works toward the individual's and the commonwealth's best interest. It is commonly accepted that private interests cannot always be represented by the individuals themselves, which is a point shared by Habermas. Individuals must establish an authority with the task of representing the interests of individuals. It remains ultimately up to individuals to determine how far the transfer of rights will stretch, and these determinations will vary depending on the context of space, culture and time.

This leads to the possibility that different manifestations of privacy, personal behaviour (personal life), personal communications and all other kinds of personal data can be restricted by ‘societal requirements’ which may also differ in time culture and political situation. This is, according to the Charter of Fundamental Rights of the European Union, only possible under the principle of proportionality, and if the requirements are necessary and genuinely meet objectives of general interest recognised by the Union or for the protection of the rights and freedoms of others. In the next chapter, the specifications of these requirements are discussed.

The last status report of the continuing story of the European data protection is a clear example of the changing tides for balancing between individual rights and public interests, which is considered the extension of the purpose element in big data processing in Chapter II in the concept Regulation:

'Such an approach, which conflates the notions of legal basis and further processing for compatible purpose, contradicts the EU data protection acquis and would be illegal under the current legal framework. It could furthermore have no other consequence but to undermine the whole new data protection framework and to dilute the level of protection for EU citizens in comparison to Directive 95/46/EC in force'.[142]

It can be concluded that there is an elasticity of privacy in both historical and cultural perspectives. This accounts for the relatively short period in the process of the negotiations on developing the General Data Protection Regulation and the Judicial Data Directive, where we see the shifting of boundaries according to the political climate of the times.

In the next chapters these boundaries are explained on the basis of the evolved conception of privacy as well as on accepted requirements for legitimised intrusion into the privacy of natural persons.

[142] Press release WP 29 , 17th March 2015 (http://bit.ly/19l7eXV)

3 Limiting Human Rights: From Exceptional Circumstances to General Conditions

3.1 Introduction

The subject of this thesis is to evaluate the modification or reduction of privacy by governmental authorities.

This evaluation can only be carried out properly if it is clear under what circumstances fundamental rights can be minimised or discarded by authorities and what legal constraints apply.

The questions answered in this chapter are:

How does the (inter)national legal framework on human rights allow for governments to limit privacy?
What principles govern the exceptions to privacy in this respect?

First, I will explain how and on which grounds, the control of the individual over his personal live and information can be transferred to governmental authority, then I will explain these grounds and under what circumstances they will apply. Finally, I will look into the legitimacy of these grounds and when the limitations will be acceptable.

3.2 Transfer of Fundamental Rights, Specifically Privacy

This dissertation asserts that fundamental rights are, first and foremost, directly connected to individual citizens. As such, these rights ought not to be transferred to national governments without the explicit consent of the individual citizen. The specific choice by these citizens to transfer the control is based on the improvement of the common good. As discussed in preceding chapters, there is inconsistency in the understanding, application and protection of fundamental rights as well as the possible limitations.

I will refer to the circumstances when and why the limitation of this right would be acceptable.

This requires a transparent set of rules and comprehensible description of the circumstances that justify a reduction or stifling of privacy in order to equalize the balance between the positions of the citizen towards the State as keeper of the common good.

At least there should be a sharp line between what rights citizens can transfer to the state and what rights should never fall within the competence of national government. In theory and also in practice this line is blurred. It must be made clear where and under what circumstances the powers of the sovereign states are limited or might be extended. The main issue is whether this transfer of individual autonomy to the state may take place under specific circumstances. If so, what might these specific circumstances that justify this transfer of individual autonomy look like? To answer this question, arguments presented by leading

scholars as Agamben, Schmitt, Habermas and Lyon on the transfer of fundamental rights to a sovereign authority will be explicated and criticized when appropriate.

In his *Political Theology* Carl Schmitt (1922) established the essential proximity between sovereignty and the state of emergency. Carl Schmitt, the 'third Reich crown jurist', indicated that it should be the State's prerogative to define where the state could override fundamental rights of its citizens. In particular, Schmitt argued that if state sovereignty is endangered, the state of exception could be invoked, calling for the overriding of individual rights.[143]

Agamben, builds on Schmitt but argues that sovereignty *is* the permanent possibility of a state of exception/emergency, wherein juridical rules can be suspended because they do not apply properly. It's the sovereign that decides whether the normal situation exists or whether there is a state of emergency.

Agamben stated that the state of emergency produced the concept of homo sacer, a citizen deprived of his civil and fundamental rights, because of the decision of the Plebiscite as punishment to the subject's criminal behaviour.[144] Subjects, individuals, are constituted by virtue *of* this very system. It is this constitution by the system that allows him to introduce the polar-opposite *homo sacer* figure who may be subject to the violence of the law of the sovereign.

In his view, national security is the ultimate excuse for governments to limit the fundamental freedoms of citizens. The dangers of the actual undermining of the moral and legal existence of the State are recognized. If there are no circumstances that can be compared with the situation as described as 'State of Exception' these measures may not be invoked. Although even within the clearer situation of a 'State of Exception' and 'State of Necessity' it has to be certain if this situation exists:

'it is to ascertain with complete clarity when a situation of necessity exists, nor can one spill out, with regard to content, what may take place in such a case when it is truly a matter of an extreme situation of necessity and of how it is to be eliminated'.[145]

This foggy way of decision making to ascertain complete clarity, is comparable with the decision to enact a situation in which a limitation of human rights, in casu privacy, may be invoked on grounds of national security. For example, after the attacks of the World Trade Centre on 9/11 it seems that there is a 'continuous state of emergency' on a worldwide scale or at least a situation of necessity in which parliamentary control is limited to the outer boundaries of what in a democratic society is deemed acceptable.[146]

---

[143] Interesting is that Schmitt also stated: '*If the constitution of a state is democratic, then every exceptional negation of democratic principles, every exercise of state power independent of the approval of the majority, can be called dictatorship.*'Carl Schmitt (1922, p. 22)

[144] G. Agamben, *The Sacred or Accursed Man, Agamben, in Homo Sacer: Sovereign Power and Bare Life* (originally published as: Homo Sacer. Il Potere Sovrano e la Nuda Vita, Giulio Einaudi editore s.p.a. 1995), California: Stanford University Press-Stanford, p. 47.

[145] At p. 55, citing Schmitt 1922.

[146] For instance for tapping of telecommunication no permission of the political responsible minister is necessary concerning the competence in tapping of the National Security Agency AIVD, Article 25-27 WIV 2002 tapping. See the supervisory commission on the national security agencies report 2009, CTIVD nr. 19, <www.ctivd.nl/?download=CTIVD%20rapport%2019.pdf>.

National security becomes the crucial element of the justification in the surveillance society. The content of the individual right concerning the respect for private life, and all the data that can be derived from that, is seen as an instrument to enhance this security. Huge amounts of personal data are the ammunition used in homeland security to defend the national interests. As Lyon states, privacy can be considered as balancing individual interests with societal interests. Embracing the rationalistic approach of the surveillance society in a very positive interpretation, Lyon recognizes the benefits of surveillance in potentially thwarting terrorism, reducing fraud and preventing crime. Privacy is considered just one value amongst others, though certainly not a dominant one.[147]

3.3 The Concept of Citizen towards the State According to Habermas

The relation between the (state) authorities and the individual citizen is essential to determine the range of intrusion that evolved in international regulations concerning the protection of individual fundamental rights. We need a theoretical background to measure and explain the changing values in this concept where the state has a role as a defender of these values but at the same time a violator who seeks to bend the rules for the sake of national security concerns and the 'war against terrorism'.

This leads us again to Habermas who uses an interesting concept in his theory of the relation between the citizen and the state.[148] In this concept there is hardly a difference between a state of emergency that asks for exceptional rules and a 'normal situation', contrary to the theory of Agamben. As I have stated above, concerning the political, policy and regulatory measures taken by the (mainly) western authorities, the distinction between 'normal' and 'exceptional' has become blurred after 9/11 and the later terrorist attacks in London, Madrid, Paris and Brussels. There is a continuous state of heightened vigilance in which the state requires (and sometimes rewards) the active participation of the citizen.[149] This resembles the orientation that has been proposed by Habermas.

According to Habermas, one can differentiate between liberal and republican concepts of Citizenship. This differentiation is not referring to situations of emergency or special circumstances but more to the contents of the concept of citizenship and the responsibility of government towards this citizenship. Dividing this separation into negative and positive rights, the citizen has certain rights that may be claimed against governments. Government can (more or less) freely decide how to limit these rights. In the words of Habermas, the liberal view defines the status of citizens primarily by negative rights against the state and other citizens. As bearers of these rights, citizens enjoy government protection as long as they pursue their private interests within the boundaries set by legal statutes. This includes

[147] Lyon 1994, p. 193.
[148] Habermas 1996, pp. 270-271.
[149] As an interesting example reference can be made to the policy development that is based on the governmental agreement 2010 (Regeerakkoord) between The Netherlands governmental parties (CDA and VVD, supported by PVV) by which a re-consideration of the concept of excessive justified self-defence, ultimately leading to a kind of anarchism that has to be restrained by the appointed government: '*That in the state of Nature every one has the executive power of the law of Nature—I doubt not but it will be objected that it is unreasonable for men to be judges in their own cases, that self-love will make men partial to themselves and their friends; and, on the other side, ill-nature, passion, and revenge will carry them too far in punishing others, and hence nothing but confusion and disorder will follow, and that therefore God hath certainly appointed government to restrain the partiality and violence of men*' - John Locke, cf. Ter Voorde 2011.

protection against government interventions that exceed statutory limits. Habermas provides no proposal as to how this excess could arise, nor how it could be prevented and how reinvestment of the fundamental right for the citizen can be guaranteed. What remains appears to be a continuous (legal) battle between individual citizens amongst each other and against the governmental authorities, to protect their rights and resist - and therefore minimise - intrusions.

In explaining this liberal structure Habermas seems to underestimate the fact that the absolute weight of power is an intrinsic element of the value of maintaining the right and the execution of the power. The weight and execution of the power of rights substantially differ between government and the citizen. To simplify this incongruity to claim protection against governmental intrusion and the 'weight of power' that shapes the exercise of government power Habermas combines all legal and political rights into private rights (civil law). These private rights create a common political will and policy in which every private person is represented. He explains this by stating that:

'Political rights have not only the same structure but also the same meaning as private rights that provide a space within which legal subjects are free from external compulsion. They give citizens the opportunity to assert their private interests so that, through elections, through the composition of parliamentary bodies and the selection of Government leaders, these interests finally aggregate into a political will that has an impact on the administration. In this way, citizens can, in the role of voters, supervise the exercise of governmental power so that it responds to the interests of citizens as private persons'.[150]

It is interesting to see that Habermas seems to have a preference for the republican view that is built on the positive concept of self-determination. In this view no rights are transferred to a public authority, but the citizen is always in charge and determines if and how these rights are exercised.[151]

He continues by stating that the surveillance society means the surveillance of the citizens themselves, wherein fundamental rights are positive rights and the reduction of these fundamental rights are positive actions of the citizen to regulate his own society:

'To this extent, the political process does not, just serve to keep government activity under the surveillance of citizens who have already acquired a prior social autonomy in the exercise of their private rights and pre-political liberties. Nor does it function as a hinge between State and society, for administrative power is by no means autochthonous; it is not something given. Rather, governmental authority derives from the power produced communicatively in the civic practice of self-determination, and it finds its legitimation in the fact that it protects this practice by institutionalizing public liberty'[152]

[150] Habermas 1996, p. 270.

[151] Idem.: *'According to the republican view, the status of citizens is not patterned on negative liberties to whichthese citizens can lay claim as private persons. Rather, civil rights –pre-eminently, rights of political participation and communication- are positive liberties. They guarantee not freedom from externalcompulsion but the possibility of participating in a common practice through which citizens can first make themselves into what they want to be: politically autonomous authors of a community of free and equalpersons*

[152] Idem.

Habermas is rebuilding Rousseau's 'Social Contract' in a more liberal way with more continuing responsibility for the individual. The protection of individual rights provides the prominent justification for governmental surveillance, which in theory may be acceptable but in practise faces insurmountable challenges. The sum of individual rights forms the common denominator on which governmental surveillance is based. It is impossible for individuals to have a continuous grip on the exercise and execution of the sum of rights and therefore also on the protection of these rights by way of the political system and governmental authority. It is interesting to note that the fears and doubts pertaining to the control mechanisms that are prevalent in the digital society, for example a fear of losing control over personal and governmental information, are not to be found in the Habermasian approach. This is because Habermas has the opinion that all citizens already agreed upon the common good. [153]

Thus, more is required of the republican citizen than just an orientation towards individual interest. He has a social responsibility for which the authority will be the representative and executive. The state is the guarantee that his rights will be transferred in norms. Norms are considered important because on their turn they create the guarantee that the rights will be executed on an equal basis for all citizens.

But, if we consider the natural legal person as bearer of private rights, what is the public law enforcement based upon? Habermas,[154] following the liberal view of Locke, states that the legal order is meant to make it possible to determine in each case which individuals are entitled to which rights. Such a system may allow for the programming of the government to account for all individuals in a 'market structured network' of interactions resulting in political goals that serve the 'commonwealth'. So the sum of all rights (including the fundamental rights) create the political and legal power of the authorities of a society. In the republican view, these 'subjective' rights owe their existence to an 'objective' legal order that both enables and guarantees the integrity of an autonomous life based on mutual respect. To be sure, republicanism at least comes close to this concept of law, which puts the integrity of the individual and his liberties on a par with the integrity of the community in which individuals are first able to mutually recognise one another both as individuals and as members of the community. Republicanism binds the legitimacy of laws to the democratic procedure governing their birth or genesis as Habermas describes it, and thus maintains the internal connection between the people's practice of self-determination and the impersonal rule of law. It is a more non-critical acceptance of a normative structure and does not give much opportunity to criticism or even reflection on the value of the normative structure:

'For republicans rights ultimately are nothing but determinations of the revailing[155] political will, while for liberals some rights are always rounded in a 'higher law' of trans political reason or revelation… In a republican view, a community's objective, the common good, substantially consists in the success of its political endeavour to define, establish, effectuate and sustain the set of rights (less tendentiously laws) best suited to the conditions and mores of that community, here as in a contrasting liberal view the higher-law rights provide the

[153]These fears are completely non-existent in this republican theory as Habermas explains it:
Stating the State's 'raison d'être' does not lie primarily in the protection of equal private rights, but in theguarantee of an inclusive opinion and will-formation in which free and equal citizens reach an understandingon which goals and norms lie in the equal interest of all Habermas 1996, p. 271.
[154] Habermas 1996, p. 21.
[155] Probably meant prevailing?

transcendental structures and the curbs on power required so that pluralistic pursuit of diverse and conflicting interests may proceed as satisfactorily as possible.'[156]

Whereas the liberal view tends toward a transcendent set of norms, the republican view is more suited to seeing out the promises of individual rights. Though this observation does not imply flexibility for adaptations to a changing society. The liberal view seems to have an almost religious conviction with remnants of Locke and Rousseau. The vision is going beyond the factual circumstances of a governmental authority that, indeed, is struggling within a pluralistic legal world. In governments pursuit of diverse interests this can substantially differ from the legal interests of the citizen. This is stated by Habermas, citing Carl de Savigny in the sense that a legal relation secures

'*the power justly pertaining to the individual person: an area in which his will rules, and rules with our consent*'.

These rights, 'in the subjective sense' are legitimate per se because, starting with the inviolability of the person, it is supposed to guarantee 'an area of independent rule' (Herrschaft) for the free exercise of the individual will.[157] This common 'free will' results in norms that secure the exercise of rights for every citizen in the same way on basis of equality of all.

This general and still applicable rule in German legal conviction - and not just there - is based upon Kant, relating to his 'principle of right' (Rechtprinzips), in which rights hinge on the freedom of choice and the person's autonomous will and their compatibility with the rights and freedoms with others to exercise the same rights.

In the end these rights, though, have to be confirmed in, and accepted by, a legal order.[158] Habermas gives an excellent overview of those different views of highly esteemed legal theorists. But one question remains: what will be the role of the individual bearer of rights in the real (legal) world? For instance, in the Charter of Fundamental Rights of the European Union in Article 7 and 8 as well as in Article 13 concerning the respect for personal life, personal data and the freedom to hold or express personal information can be restrained by objectives of general interest, generally set in Article 52 of the Charter. Although referring to the Convention on the Protection of Human Rights and Fundamental Freedoms, a more extensive protection by the Charter is not excluded.[159] So a possible restriction of the limitation of privacy by governmental authorities as such is deemed possible. It would be surprising if European Union law, in for example the Privacy Directive or the proposed General Data Protection Regulation, would move beyond the 'normal' principles because categories of proportionality and subsidiarity could/would support this exception.

---

[156] Idem, p. 271.
[157] Habermas 1998, p. 126.
[158] For further references to the autonomous individual rights theories, referring to Kelsen, Ihrering, Hobbes, Kant, etc. see Habermas, 1998 p. 85 – in a reconstructive approach to the law: Chapter 3.
[159] Charter of Fundamental Rights of the European Union Official Journal of the European Communities C 364/1, December 18, 2000:
Art. 52.3. 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.

3.4 Restrictions or Limitations

So what happens in the real world outside the theorist's conceptions? National authorities, as public actors, will strive for at least a considerable control over the exercise of their powers under all circumstances, especially if their sovereignty is tested. States will never totally give up parts of their sovereignty, even in the case of unalienable fundamental rights. In the process of negotiating international conventions there must be the possibility to pursue different national interests, be they economic or pertaining to security. Nation states will never give up interior control. So even the most fundamental rights abiding democratic state must preserve that right to limit the fundamental rights of its citizens to preserve the security of the state or even the economic well-being.

The limitations can be relative though, based on the political system of that state, but nevertheless there always may occur circumstances within the general interests of that state that ask for postponement of the exercise of fundamental rights of its citizens. Nevertheless, limitations will always be an intrinsic aspect of the international instruments that guarantee (non absolute) fundamental rights.

Conventions and other instruments may contain a number of restrictions or limitations to the rights they stipulate. It is generally accepted that only a few rights and freedoms are 'absolute'. It is important that exceptions as stated in the international laws, as in Article 8(2) of the European Convention on Human Rights and the articles mentioned hereunder, must only be used by national authorities to establish the proper limits of the protected right, and not as an excuse for undermining the right itself or destroying it altogether. In general, there must be a legitimate and proportional relationship between the restriction of the right as such and the reasoning provided for the restriction.

Various international instruments contain provisions allowing restrictions (used interchangeably with the term 'limitations') on human rights. Such provisions may take the form of general limitations. Article 4 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), for instance, reads:

'The states parties to the present Covenant recognise that, in the enjoyment of those rights provided by the State in conformity with the present Covenant, the State may subject such rights only to such limitations as are determined by law only in so far as this may be compatible with the nature of these rights and solely for the purpose of promoting general welfare in a democratic society.'[160]

Another illustration is provided by Article 32 (2) American Convention on Human Rights (ACHR):

'The rights of each person are limited by the rights of others, by the security of all and by the just demands of the general welfare, in a democratic society'.

Although the right of privacy seems to be well protected in Article 11 of this Convention[161], this paragraph gives ample opportunity to 'correct' the freedoms by government to protect

[160] http://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf

[161] No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation,

security. This can be based on the exceptions within the convention as defined in national law and given the guarantees within constitutional or national law.[162]

The African Charter on Human and Peoples' Rights does not contain a specific provision on restrictions, but Article 27 (2) on 'duties' plays the role of a general limitation clause providing:

'The rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest.'

Likewise in the International Covenant on Civil and Political Rights a general derogation is made possible under times of emergency. This general exception is stated in Article 4 ICCPR and reads as follows:

'In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin'.

Although the derogation from the purpose and exercise of fundamental rights seems to be limited by 'other obligations of international law' one may wonder how 'gratuitous' such words are in the context of the rest of the text of this Article. In the international arena it is recognised, though, that the limitation has not to be interpreted too light-heartedly. In order to prevent abuse, conventions often contain a paragraph prohibiting the abuse of an international instrument to unduly infringe upon another right. Article 5 ICCPR, for instance, stipulates:

'Nothing in the present Convention may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms recognised herein or at their limitation to a greater extent than is provided for in the present Covenant.'

The United States, though, had no problem transgressing the purpose of these articles in making a bundle of reservations based upon the possibilities given in Article 4 (and even without these grounds) with the predictable result of, as eloquently described by Kristina Ash in 2005 her article on U.S. reservations in human rights,

'*render[ing] international human rights treaties impotent in U.S. law.'*[163]

Further she refers specifically to the objections of other states to the reservations of the U.S.

<http://www.oas.org/juridico/english/treaties/b-32.html>.

[162] Article 2 of the Convention: Where the exercise of any of the rights or freedoms referred to in Article 1 is not already ensured by legislative or other provisions, the States Parties undertake to adopt, in accordance with their constitutional processes and the provisions of this Convention, such legislative or other measures as may be necessary to give effect to those rights or freedoms.

[163] U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence, Northwestern University Journal of International Human Rights Volume 3 (Spring 2005).

'Countries such as The Netherlands objected to the U.S. reservation because it allegedly went against the object and purpose of the treaty. Article 4 of the ICCPR allows for derogation from the covenant during times of national emergency. However, Article 4 Section 2 prohibits States from derogating from essential articles in the Covenant. These articles include the right to life, the right to be free of torture and slavery, right to be free of imprisonment for breach of contractual obligations, right to be free of ex post facto laws, right to be recognised as a person before the law, and freedom of thought, conscience and religion. None arguably, the most essential of these articles is the right to life. By reserving the right to sentence persons under the age of eighteen to death, the United States contravened a major object and purpose of the treaty. So the fact that restrictions of fundamental rights must be within the limits of international law is not sacred either.'

But even without these reservations it seems to be not much of a problem to limit fundamental rights under threatening circumstances. It is not unthinkable that potential threats by terrorist activities require intrusion of the fundamental right of privacy, entailing the use of all kinds of personal information or intrusion of the premises of subjects.

However, apart from these general provisions of which the extent is not very well defined, most human right treaties contain various provisions, which specify the limitations and restrictions to a particular right. Such specific limitation clauses include phrases as 'prescribed by law', 'in a democratic society', 'public order (*ordre public*)', 'public health', 'public morals', 'national security', 'public safety' and 'rights and freedoms of others'. For a few rights, such as freedom from torture or slavery, no limitations have been formulated. That is the difference between so called 'absolute' and 'non-absolute' rights. Still, the fact that no limitations have been provided for, does not mean that states will not intrude those absolute fundamental rights…

In sum, any restriction on the enjoyment of the rights enshrined in human rights instruments must be legally established, non-discriminatory, proportional, compatible with the nature of the rights and designed to further the general welfare. Finally, it is also important to stress that the burden lies upon states to prove that a limitation imposed upon the enjoyment of the rights is legitimate. This is, of course, a heavy burden of proof, but consistent with the object and purpose of human rights treaties to protect the individual.

3.4.1 Limitation Rules on Fundamental Rights

Non-absolute fundamental rights, such as privacy, may be limited. That means, contrary to absolute rights where limitation is forbidden, these limitations have to be supported by the guarantees against misuse or 'detournement de pouvoir'.

When a right is subject to a limitation, the reason for its limitation should be well-defined. Moverover, any limitation must comply with the minimum requirements as indicated by

e.g.Westin, Van Dijk & Van Hoof, Morham and others, case-law from the ECtHR[164], the ECJ[165], national courts[166] and legislation.

The fact that the law, upon which the exception is based, would be useful is in itself not sufficient; it must be consistent with other protected rights. Limitation rules are always applicable and not specifically apply to a kind of emergency. As an example I refer to the Dutch Constitution (Article 103) in which circumstances of internal or external threat provide for a 'state of exception' to be formally declared by the Government. Although it is interesting to analyse the circumstances under which this state of exception will be declared, generally it is applicable on a declaration of state of war, state of occupation or so called extraordinary circumstances. On basis of these different declarations, a variable set of so called emergency laws can be declared in force.

Although it is easy to enact the exceptions in a non-formal way, without the necessity of a state of emergency, still based on rather broad motives of (perceived) threats. This is shown by the numerous regulatory initiatives that have been enacted by the western world authorities after 9/11. As an illustration I refer to the way the European Union created a legal basis for the European and national authorities to intrude upon the private life of persons, allegedly involved in suspicious money transactions.[167] The Council Regulation provides for the freezing of the funds of all persons who participate, knowingly and intentionally, in acts of terrorism or in preparation thereof. The adoption of this regulation was recognized and further developed in later Council Common Position[168] on the application of specific measures to combat terrorism, by defining the term 'terrorist act.' According to this Council Position, the definition of 'terrorist act' encompasses everything from intimidating a population to the commission of acts that cause death or harm to 'the fundamental political, constitutional, economic or social structures of a country…'[169] The European Union

[164] As in, but not restricted to: ECtHR 2 August 1984, *Malone v. UK* [1984], 7 EHRR 14. ;
ECtHR 25 March 1983, *Silver v. the UK* [1983], A. 61, paras. 97-98.;ECtHR 23 September 1982, *Sporrong and Lönnroth* [1982], A 52, s. 26, 28, paras. 69, 73. ; ECtHR, *Malone v. Metropolitan Police Commissioner* No. 2 [1979], 2 WLR 700. ;ECtHR 26 April 1979, *Sunday Times v. UK* [1979], 2 EHRR 245.;
ECtHR 6 September 1978, *Klass and others v. Federal Republic of Germany* [1978], 2 EHRR 214.;
ECtHR 7 December 1976, *Handyside v. UK* [1976], A. 24, paras 48-49. And Weber and Saravia v. Germany and Valenzuela Contreras v. Spain

[165] As in, but not restricted to: Cases C-293/12 and C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland Ltd v. Minister for Communications* [2012].; Cases C-92/09 and C-93/09, 9 November 2010, *Schecke and Hartmut* [2010], ECR I-11063; 6 October 2015
Case C-362/14 Maximillian Schrems v Data Protection Commissioner

[166] Supreme Court of The Netherlands (Hoge Raad) 28 September 2010, LJN BM6656 [2010], *NJ* 2010, 532.
Supreme Court of The Netherlands (Hoge Raad) 20 April 2010, LJN BK3369 [2010], *NJ* 2011, 222.
Supreme Court (Bundesverfassungsgericht) 15. December 1983 [1983] 1 BvR 209/83
Supreme Court (Bundesverfassungsgericht) 3 March 2004 [2004], 1 BvR 2378/98.
Supreme Court (Bundesverfassungsgericht) 2 March 2010 [2010], 1 BvR 256/08.

[167] Council Regulation (EC) 2580/2001 of December 27, 2001 on Specific Restrictive Measures Directed Against Certain Persons and Entities with a View to Combating Terrorism [2001] OJ L344/70.
[168] Council Common Position (EC) 931/2001 of December 27, 2001 on the Application of Specific Measures to Combat Terrorism [2001] OJ L344/93.
[169] See this citation of Zelman 2001.

embraced the positions taken by the UN Security Council and integrated this in the European legal framework.[170]

Organisations or natural persons placed on the 'suspicious' list, even though they are unaware of the circumstances and even do not know that they are on the list, are deprived of their rights without any democratic guarantees or the right to defend their position. And if they are confronted with the fact that they are on the list, they will have lots of trouble proving they have no terrorist intention. A positive result in using the legal remedies, though, was proven in the so called *Kadi* decision, which held that any new Regulation should be subject to the human rights protections provided for in the Community legal order, including fundamental rights as privacy.[171] The result was that the ruling of the European Court of Justice's annulled the implementation of the legislation for Resolution 1390 (2002). Further case law and comparable decisions concerning public order and security issue will be subject of the next chapter.

3.4.2 Almost Forgotten: The Siracusa Principles[172]

Most of the requirements for accepted circumstances and necessary legal guarantees in the exceptions to fundamental rights have been developed within academia and by the case law of major human rights bodies. In this regard it is interesting to introduce the almost unnoticed Siracusa Principles on the Limitation and Derogation provision in the International Covenant on Civil and Political Rights. The Siracusa Principles were adopted by a group of 31 distinguished experts in international law, convened by the International Commission of Jurists, who met in Siracusa, Sicily in 1984 and defined a set of Principles to consider the limitation and derogation provisions of the International Covenant on Civil and Political Rights. The participants agreed upon the need for a close examination of the conditions and grounds for permissible limitations and derogations expressed in the Covenant in order to achieve an effective implementation of the rule of law. As frequently emphasized by the General Assembly of the United Nations, a uniform interpretation of limitations on the rights as provided for by the Covenant is of great importance.

Although the Siracusa principles formed not the first or the last attempt to specify derogations from the protection of human rights, the Principles are open to more non-exceptional circumstances than the other sets of norms.[173]

---

[170] See Consideration 4: The European Union should take additional measures in order to implement UNSC Resolution 1373 (2001).

[171] Joined Cases C-402/05 & C-415/05, *Kadi & Al Barakaat v. Council of the European Union* [2008], 3 C.M.L.R. 41. After the Court annulled Regulation 881/2002, the Council amended it with a new regulation. Commission Regulation (EC) 1190/2008 OJ L322/25; Amending for the 101st Time Council Regulation (EC) 881/2002. For further consideration of the *Kadi* judgement and its impact, see Posch 2009.

[172] United Nations, Economic and Social Council, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, U.N. Doc. E/CN.4/1985/4, Annex (1985). Siracusa Principles: for all principles see Annex

[173] In his study: *Derogation Of Human Rights International Law Standards – A Comparative Study*, Leon Wessels describes the other set of norms that are specifically directed on the state of emergency, i.e. the Questiaux Report (1982); the International Commission of Jurists (ICJ) report (1983); the Paris Minimum Standards of Human Rights Norms in a State of Emergency report 1983 and the Oslo Statement on Norms and Procedures in Times of Public Emergency or Internal Violence, 1988; Turku/Åbo Declaration of Minimum Humanitarian Standards (1990).

It is interesting to compare these principles with measures in the European context of Article 8 (2) ECHR and the limitations within general privacy regulations, telecommunication retention, anti-terrorism and anti-money laundering regulations.

The motivation underlying the formulation of the principles was to define rules based on the assumption that the UN should realise a more coherent approach to threat and risk assessment and risk management. These principles are aimed at a broad range of disturbances of societal processes.

Surprisingly, the principles applicable to limitations in the ICCPR are hardly referenced in any other international legal instrument, though, arguably, could be applicable and used in many other limitation clauses. This idea is supported by Joan Fitzpatrick in her book 'Human rights in Crisis' where she states that the Siracusa Principles also venture into the territory of non-treaty (ICCPR) based studies and can provide recommendations to national authorities and those involved in the legislature in their review of the necessity for specific derogation measures.[174]

As developed in the following chapter, the ECHR and the ECJ have adopted these principles in their case law.

These principles could also be used to guide the development of security policies. The European Commission proposed in 2010 a set of measures to improve identification and minimize the impact of all natural, accidental and malicious threats and hazards. This is a general mandate to act in 'threatening circumstances' which are not specifically described, though nevertheless provides ample opportunities for authorities to take (restrictive) measures:

'Existing sector-specific risk assessment and situation awareness functions in the EU institutions and agencies, such as those concerning natural disasters, threats of health pandemics, nuclear risk monitoring and terrorism, should be linked up. Response to emergencies, as set out in the Commission's communication last month, is an integral part of this objective'[175]

More precisely, the antiterrorism regulations introduces extraordinary powers, in order to protect citizens against terrorist attacks, allowing the administration to reassure them of the continuous capability of the State to bridge the gap in security, at the cost of increasing the administrative control over the citizens.[176]

3.5 Derogations to Fundamental Rights as Considered Acceptable by the Siracusa Principles

Principles like the ones mentioned in the Siracusa Principles can be helpful to set the limitations on both the development and use of regulations to enhance security under circumstances that allow derogations from these 'normal circumstances' as for purposes in

[174] Fitzpatrick, p.70
[175] The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Memo 10/598.
[176] Simoncini 2009.

the protection of public security, criminal justice and anti-money laundering (AML) in the light of combating terrorism.

The Siracusa Principles are not specifically directed to the state of emergency as for instance presented by Agamben, by external threats to national and international security but refer to any disruption of the 'normal' legal climate by unexpected circumstances. This reference is not easy to interpret. How to describe 'disruption by unexpected' (i.e. not normal) circumstances? When does a disruption of a 'normal legal climate' occur? Could one say that derogation from the normal situation in which fundamental rights are respected, as described in legal instruments is a disruption as such? Or is this a 'normal' situation under different circumstances or for different purposes?

Existing regulations and for instance, in the future European framework to protect privacy, the proposal for a Regulation on the protection of personal data (General European Privacy Regulation), give ample opportunity to regulate the protection in different national legal instruments if issues of national security or criminal investigation or any justice matter occur.[177]

Long before the destruction of the twin towers on September 11 in 2001, it was agreed upon by the Nations which convened in Siracusa, that there is a limited set of circumstances and a clear set of conditions that are decisive about how and to what extent human rights can be limited in their application.[178] In all other legal instruments that create exceptions to fundamental rights one finds reference to comparable principles.

In this set of basic principles, a general interpretation is determined to justify limitations on the rights and principles as stated in the ICCPR (the Covenant).[179] This set of principles though will be useful for any legal instrument that gives the possible limitation of the right of privacy to the State.

The document divides these limitation principles in main principles and specific circumstances. Derogations are only permitted and justified as stated in the terms. The object and purposes of the Covenant are not to be interpreted as to jeopardise the essence of the right concerned. All limitations of the rights of the Covenant have to be provided for in the law and should be compatible with the Covenant.

The Principles can be considered as a specification of the State of emergency in Article 4 of the Covenant.[180] Interestingly, the Siracusa Principles are considered to be applicable to any

[177] Article 2 states that this Regulation does not apply 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.

[178] United Nations, Economic and Social Council, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, U.N. Doc. E/CN.4/1985/4, Annex (1985).

[179] International Covenant on Civil and Political Rights Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49

[180] Article 4 relates to identifying the state of emergency: 1. In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.

derogation from the fundamental rights of the Covenant, not limited to the State of emergency. The limitation of absolute fundamental rights is not allowed under whatever circumstances. [181] The more general exceptions on the freedom of information, speech and communication in Article 19 of the Covenant can be understood as a common limitation clause for non-absolute rights such as privacy or even for the application of these exceptions in general.[182] Although no specific reference is made to limitations on the right of privacy as provided for in Article 17 of the Covenant, the specified limitation of Article 19 on freedom of expression is a comparable right of informational sovereignty of natural persons, an essential element of the informational privacy, which includes the right to determine one's opinions in the medium of one's choice.[183]

The effect of the Principles is clear in the commentary of possible limitation of this right.[184] More importantly, the Siracusa Principles give the specific circumstances and preconditions under which a derogation of the agreed civil and political rights is possible. This reasoning can directly be applied to any limitation to non absolute fundamental rights as privacy. The general principles are enumerated in the considerations of the first paragraph, the limitation clauses:

'No limitation referred to in the Covenant shall be applied for any purpose other than that for which it has been prescribed'.

This seems to be very logical, but practise reveals this clause has been continually disregarded in several national and international regulations that tend to give room for 'function creep'.[185] This risk is to be provided for in a clear description of the point of departure for a possible limitation of a right recognized by the Covenant. The necessity of the limitative measure should be motivated in a clear way, based on specific grounds and within defined circumstances.

'No limitation shall be applied in an arbitrary manner. Every limitation imposed shall be subject to the possibility of challenge to and remedy against its abusive application.

---

[181] 2. No derogation from articles 6, 7, 8 (paragraphs I and 2), 11, 15, 16 and 18 may be made under this provision.

[182] Article 191. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this Article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

[183] Article 17: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

[184] The HRC in its General Comment 34 has emphasised that: *'when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself...the relation between right and restriction and between norm and exception must not be reversed.'* Also see the report of the European Centre for Law and Justice <http://eclj.org/pdf/eclj_draftgeneralcommentno34-article19_20110201.pdf>.

[185] For instance, reference is often made to protection of personal information within a certain structure as police investigation or national security, all to strengthen democratic society. A clear national example is the applicability in the Dutch Act on Police Data where limitation is phrased in the sense of description of personal data as police data whenever it is to be processed within the police task. This automatically results in non applicability of general privacy laws. The data can be used for any purpose within this task, be it the specific case, comparable studies or any other purpose within the competence of the police. This would be contrary to the first principle.

No limitation on a right recognized by the Covenant shall discriminate contrary to Article 2, paragraph 1.

Whenever a limitation is required in the terms of the Covenant to be 'necessary,' this term implies that the limitation:

(a) is based on one of the grounds justifying limitations recognized by the relevant Article of the Covenant,
(b) responds to a pressing public or social need,
(c) pursues a legitimate aim, and
(d) is proportionate to that aim[186]

Any assessment as to the necessity of a limitation shall be made on objective considerations. In applying a limitation, a State shall use no more restrictive means than are required for the achievement of the purpose of the limitation.

The burden of justifying a limitation upon a right guaranteed under the Covenant lies with the State.

The requirement expressed in (Article 12 of) the Covenant, that any restrictions be consistent with other rights recognized in the Covenant, is implicit in limitations to the other rights recognized in the Covenant.

The limitation clauses of the Covenant shall not be interpreted to restrict the exercise of any human rights protected to a greater extent by other international obligations binding upon the State'.

Thus these Principles must be applied consistently with the terms as expressed and explained within the Covenant. These limitation clauses can be found in most international legal texts in Treaties as well in case law. I will later discuss relevant cases of the ECtHR in this respect.

The controversial element in these Principles, is that on the one hand there is a reference to the rights that are to be protected in the Principles referring to the UN ICCPR, but those rights are rather limited in their description. On the other hand the actual coverage of the Covenant is considered broader. As already commented by Robertson[187] in 1968 in a comparison between the European Convention and the comparable UN instruments, he concluded that both instruments breathe a spirit of comparable attitude.[188] This means that although the Principles are of the same character, the wording of the more global instruments are naturally of a more general nature. Indeed, concerning privacy, the description of this principle is even wider in the ICCPR where Article 17 goes beyond the description of privacy, family, home and correspondence by also mentioning honour and reputation.[189]
The Principles are set out the ultimate purpose of law with reference to Article 29 (2) of the Universal Declaration of Human Rights:

---

[186] Comparable with: ECtHR April 26th, 1979, *Sunday Times v UK* [1979], 2 EHRR 245.
[187] J. Lavery, P. Johnston & S. Ludwin, *Proposed Amendments for Public Emergencies in the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* 2008, <http://www.pre.ethics.gc.ca/policy-politique/initiatives/docs/Public_Emergencies_March_2008_-_EN.pdf>.
[188] Robertson 1968, p. 23.
[189] Robertson 1968, p. 30.

In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

The essence of the requirements to limit the human rights and specifically privacy, lies in the specification of the grounds that are used for the restrictive measures. It is one thing to mention these grounds; it is something different to apply these principles in the decision to limit the fundamental rights on these grounds. How is a measure proportional to its goal if the goal is not exactly clear?

It was recognised by the delegates convened to negotiate the Siracusa Principles that there is an imminent danger that security issues may be hampering fundamental rights in an unacceptable extension.[190]

The participants agreed that:

(a) There is a close relationship between respect for human rights and the maintenance of international peace and security; indeed the systematic violation of human rights undermines national security and public order and may constitute a threat to international peace.

In the first place it must be clear to the natural person (legal subject) that limitations that can be considered as intrusions on his fundamental rights are known, are possible within the legal system and are clear to the persons concerned. Further, it has to be made clear under what circumstances these intrusions are permissible. On top of that, it must be clear to the legal subject that there are remedies to an accountable authority if s/he does not agree with this limitation.

In order to consider whether the reduction of privacy by governmental authorities in the context of criminal investigation, security and public order is ever acceptable, we have to look into the requirements that must be fulfilled before such a limitation or intrusion of this fundamental right complies with international legal standards. Although all of the 'holy six' reasons for limitations are described in the Covenant and Principles,[191] I will only comment on the principles relevant for this thesis. These principles also return in the relevant deliberations within the case law of the European Court of Justice and the European Court of Human Rights.

3.5.1 'Prescribed by Law'

No limitation on the exercise of human rights shall be made unless provided for by national law of general application which is consistent with the Covenant and is in force at the time the limitation is applied.

---

[190] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, September 28, 1984, E/CN.4/1985/4, available at: <http://www.unhcr.org/refworld/docid/4672bc122.html>.

[191] Public order, national security,public safety, public health, public moral, rights and freedom of others and public trial

General application in this sense, has to be referred to as national law on the highest level, as in The Netherlands, law in a formal sense, approved by Parliament. It would not be acceptable to use lower (administration) regional rules in limiting the fundamental freedom of citizens. Nor would it be acceptable to enact non-transparent or temporal regulations to justify the limitation of rights.

Questions can be raised at the transparent and temporal aspect of the so called 'special' laws based on perceived threats by terrorism as can be recognized in the US Patriot Act, an artificial acronym with the almost poetic name: 'the Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001'.[192]

Directly after '9/11' American scholars voiced their doubts about the 'privacy sustainability' as a dangerous trade-off between privacy and security.[193] These doubts were confirmed in January 2014 in a report on the application of this Act on retention and interception of telephone communications records.[194] The same confirmation is found in the European counterparts, resulting in the annulment of retention regulations as amply described later in this book.

Logically, there are more aspects of the concept of the law that have to be described. The law has to be understandable and accessible for the persons it concerns, i.e. the citizens as also described in the Principles.

Laws imposing limitations on the exercise of human rights shall not be arbitrary nor unreasonable.

Legal rules limiting the exercise of human rights shall be clear and accessible to everyone.

The tendency has nevertheless been, as in the Netherlands and in other states, to increase the use of technologies to intrude privacy.[195] For example, The Netherlands Intelligence and Security Services Act (NISSA),[196] which governs the secret service of the Netherlands, states that information may be processed in the light of the task as foreseen in the law. These activities must be reported by the responsible Department Minister (of interior) to the Parliament. However, the content of this report may be limited on basis of secrecy.[197] Additionally, paragraph 13.1.c; 36 NISSA permits the transfer of any information of a Dutch or any national person to foreign information services.[198] The transference of such

[192] Pub. L. No. 107-56, 115 Stat. 272.
[193] Heymann 2001.
[194] Privacy and Civil Liberties Oversight Board: *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,* January 23, 2014 [https://www.documentcloud.org/documents/1008957-final-report.html]
[195] Rathenau institute (2008) in the report: *From Privacy Paradise to State of Control*
[196] National Intelligence and Security Servuices Act of 7 Februari, 2002 (Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002).
[197] Article 8 S.S.A.1. Our involved Ministers will yearly report to the Senate and Parliament a public report about the manners of operation of the last year of the National Intelligence and Security Agency (AIVD) and the Military Intelligence and Security Agency.
(Onze betrokken Ministers brengen jaarlijks voor 1 mei gelijktijdig aan beide kamers der Staten-Generaal een openbaar verslag uit van de wijze waarop de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst hun taken in het afgelopen kalenderjaar hebben verricht.)
[198] Article 13.1. c. concerning a person that is subject to research in other States.(…) omtrent wie dat noodzakelijk is in het kader van het onderzoek betreffende andere landen. And Article 36 NISSA: d: If

information need not be disclosed to Parliament if it would reveal secret sources or sources from international information agencies.[199] What we see is an inclination to 'secret' non-transparent rules and policies which risks entailing legal uncertainty for the citizens. This is stressed moreover if it considers the role of information agencies and pre-prosecuting investigation of police authorities in exchanging information.

The right recommendation would be to create a neutral institution tasked with deciding on the just application of the aforementioned rules, just as advocated in the following principle, as was also required in the 'Retention Directive decision' of the ECJ.[200]

Adequate safeguards and effective remedies shall be provided by law against illegal or abusive imposition or application of limitations on human rights.

Further, it is stated in the Siracusa Principles that the principles have to be derived from a political statute that has to be considered democratic. Logically, the legal framework that allows authorities to limit the fundamental rights must have permission to do so on the basis of a mutually agreed upon democratic procedure of law-making. This means that the principles that have to be applied in societies that are not considered democratic, are not applicable. This poses a difficult juxtaposition. Should non-democratic states be expected to apply principles that are established in democratic systems? In Article 21, as stated hereunder, a very pragmatic solution is applied to adress this problem. The remaining questions are: is UN membership and adherence to the Charter and the Declaration of Human Rights sufficient to guarantee this? Secondly, what might the value of a declaration of using no limitation of the rights beyond that line, be in a State that does not abide by the UN Charter?

3.5.2 'In a Democratic Society'

The expression 'in a democratic society' shall be interpreted as imposing a further restriction on the limitation clauses it qualifies.

The burden is upon a State imposing limitations so qualified to demonstrate that the limitations do not impair the democratic functioning of the society.

While there is no single model of a democratic society, a society which recognizes and respects the human rights set forth in the United Nations Charter and the Universal Declaration of Human Rights may be viewed as meeting this definition.

The reasons for limiting of fundamental rights can be found in protecting situations that would impair the 'holy six': public order, public health, public morals, national security, public safety and, the rights of others. This thesis concentrates on public order, including crime fighting and national security. Therefore, it is of the utmost importance to define what is considered public order and security. Those definitions are the basis on which limitation of

necessary within the task are allowed to transfer information to foreign security agencies. (Daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen.)

[199] Article 9 NISSA

[200] Cases C-293/12 and C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland v. Minister for Communications,* see Chapter 5

the right on privacy is legally approved. It is interesting that public order is to be conceived as the whole set of principles upon which society is founded, including fundamental rights. However to protect these very rights, one must concede, to an undefined degree, to intrusion into these rights.

3.5.3 'Public Order (Ordre Public)'

The expression 'public order (ordre public)' as used in the Covenant may be defined as the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded. Respect for human rights is part of public order (ordre public). Public order (ordre public) shall be interpreted in the context of the purpose of the particular human right which is limited on this ground.

State organs or agents responsible for the maintenance of public order (ordre public) shall be subject to controls in the exercise of their power through the parliament, courts, or other competent independent bodies.

Although the description in the Siracusa Principles document is of a high ideological level, the practice of interpretation and application, i.e. the execution of measures in light of the protection of public order, is more connected to the concept of security than to 'respect of the (human) rights of the public'. The remaining difficulty is that the criteria for the authority to invoke the state of exception are not adequately accounted for in the legal documents that are describing the State of Exception concerning public order. This State is defined as the policy to react on acts that endanger the public good:

'the governing policy within a community as embodied in its legislative and judicial enactments which serve as a basis for determining what acts are to be regarded as contrary to the public good'.

This reasoning as reaction for derogation to adhere to the 'normal status' of fundamental rights seems unacceptable in a 'democratic' developed society and indeed forms a 'contradictio in terminae' because the public moral should always be that derogation from fundamental human right in se, is not acceptable in this society. This definition seems to define solely the acts that will endanger society, in this way including the fundamental rights as part of the public good.

3.5.4 'National Security'

National security can be considered the most undefined yet is the most frequently invoked reason of national governments to limit fundamental rights of its citizens. There hardly is any limit to the reasoning of what is permitted if national security is endangered. [201]

[201] An alarming example of extension of moral borders can be found in a Dutch report of the Supervisory Committee on the National Security Intelligence Services (CTIVD) in 2014 considering the source and origin of the information obtained by the intelligence services:*On basis of human right treaties and the constitution must the intelligence agencies refrain from information acquired by torture or by information from foreign intelligence services if there are clear indications that those methods are used. Only in emergency situations are the national intelligence agencies permitted to deviate from this principle. In practice though, it will be virtually impossible to determine if the information of foreign agencies is obtained by torture.*

The principles define the situation of endangering the life of the nation quite clear. Only then 'derogation' from the rights in the Covenant is deemed possible:

A State party may take measures derogating from its obligations under the International Covenant on Civil and Political Rights pursuant to Article 4 (hereinafter called 'derogation measures') only when faced with a situation of exceptional and actual or imminent danger which threatens the life of the nation. A threat to the life of the nation is one that:

(a) affects the whole of the population and either the whole or part of the territory of the State, and
(b) threatens the physical integrity of the population, the political independence or the territorial integrity of the State or the existence or basic functioning of institutions indispensable to ensure and project the rights recognized in the Covenant.

Internal conflict and unrest that do not constitute a grave and imminent threat to the life of the nation cannot justify derogations under Article 4.

Taking into account the existing or perceived terrorist threats, numerous anti-terrorist and anti-criminal regulations and national laws have passed the constitutional gates of national parliaments and international assemblees. The Principles are quite clear on the boundaries to the limitations and try to explain how far and to what extent this reasoning stretches. The remaining problem is one of interpretation and applicability of the rules and circumstances. The mentioned 'vague and arbitrary limitations' are inherently difficult to define because each authority will have another interpretation of the terms. National security may be invoked when the continuity of the state is endangered. But when is the continuity endangered? By terrorist threats? By computer crime activities originating from other states?

'National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.

National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.

National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.

The systematic violation of human rights undermines true national security and may jeopardize international peace and security. A State responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population'.[202]

(Op grond van internationale mensenrechtenverdragen en de Grondwet dienen de AIVD en de MIVD zich bovendien te onthouden van het gebruik van informatie van buitenlandse diensten indien er concrete aanwijzingen bestaan dat deze door marteling is verkregen. Slechts in zeer uitzonderlijke noodsituaties mogen (of zelfs moeten) de diensten hiervan afwijken. In de praktijk blijkt het voor de diensten echter vrijwel onmogelijk om in concrete gevallen te achterhalen of informatie die afkomstig is van een buitenlandse inlichtingen- of veiligheidsdienst door foltering is verkregen p. 86/87 CTIVD rapport nr. 38.
[202] Par. 29-32.

If there are no circumstances that can be compared with the situation as described as a 'State of Exception', then these measures may not be invoked.[203] The problem is, of course, that these exceptional circumstances are not well defined either. It all depends on the policies and political circumstances of that moment. Are the circumstances revealing an exceptional threat of invasion by another state or befriended states? Is the state of exception growing into a 'normal' situation?

This foggy description of those circumstances, dependent on the state of mind of politics determines the decision to enact a situation in which a limitation of the human rights, in casu privacy, may be invoked on grounds of national security.

3.5.5 'Public Safety'

In considering activities of the police, public safety is rather well-defined in national law. However, the limitation of privacy on the basis of public safety (and public order) is often not completely clear and is sometimes combined with national security issues. Therefore, both the means that are used to solve crimes against public safety and the measures to protect public safety in general make use of means that may limit the liberties of privacy. The US Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals states that the means used to limit privacy must be fair:

'*As surveillance technologies have expanded the technical capability of the government to intrude into personal lives, the law has sought to maintain a principled balance between the needs of law enforcement and democratic freedoms'.*[204]

The actual safeguards as mentioned under the following paragraph are regrettably not always in place to test this balance of fairness.

'Public safety means protection against danger to the safety of persons, to their life or physical integrity, or serious damage to their property.

The need to protect public safety can justify limitations provided by law. It cannot be used for imposing vague or arbitrary limitations and may only be invoked when there are adequate safeguards and effective remedies against abuse.'

In these paragraphs[205] the importance of adequate safeguards and clear limitations of the arbitrary competence is recognized. In paragraph 34 there is a concealed warning against confusing sovereignty of the state authority with the power and just capacity to use these powers in the exercise of measures based on its own laws.

---

[203] Although even within the clearer situation of a 'State of Exception' and 'State of Necessity' there are always doubts if the situation exists as such. *'it is to ascertain with complete clarity when a situation of necessity exists, nor can one spell out, with regard to content, what may take place in such a case when it is truly a matter of an extreme situation of necessity and of how it is to be eliminated'.* Agamben 2005, p. 55; citing Schmitt 1922.

[205] Par. 33 and 34.

3.5.6 'Rights and Freedoms of Others' or the 'Rights or Reputations of Others'

This limitation that is often referred to in the case law of the European Court on Human Rights is less relevant for the discussion of privacy. Although the sum of rights and freedoms of others may be used to limit privacy by means of legal instruments, the purpose usually seems to be more positive. The use of a fundamental right cannot impede the rights of others, including their reputation. This requires a continual balancing of interests.

'The scope of the rights and freedoms of others that may act as a limitation upon rights in the Covenant extends beyond the rights and freedoms recognized in the Covenant.

When a conflict exists between a right protected in the Covenant and one which is not, recognition and consideration should be given to the fact that the Covenant seeks to protect the most fundamental rights and freedoms. In this context special weight should be afforded to rights not subject to limitations in the Covenant.

A limitation to a human right based upon the reputation of others shall not be used to protect the State and its officials from public opinion or criticism'.[206]

This last paragraph is interesting in light of this research because it can be connected to the misuse of protective powers of certain governmental authorities, going beyond the 'normal' use of the individual rights as protection of reputation in the light of privacy protection. The safeguards that have to be defined by democratic institutions as the parliament are very important in this respect. The Anglo-Saxon system of injunction, super-injunction and hyper-injunction gives the possibility of a court ruling to 'protect' natural persons from intrusion in to one's personal life by publication bans. On the other hand, this also blocks any fundamental rights of information gathering and freedom of expression and even the discussion of the subject in parliament.[207]

To conclude this description of principles which are considered of importance in deciding under what circumstances limitation of privacy is acceptable, it would be a copout to state the obvious: that the circumstances vary over time, culture and subject. Indeed, it is always a matter of finding the right balance between the interest of one or a few against many. This involves the weighing of a non-absolute fundamental right, i.e. privacy, against an umbrella interest, such as national security. The system of weighing is interesting because the principles on both sides are not absolute. This also accounts for the description of terminology as public order and national security, terrorist crime, etc. As will be shown later, it will be difficult to find unambiguous solutions in this balancing act. This means that an easy scheme of application of the principles is not possible.

As Helen Nissenbaum stated:

---

[206] Par. 35-37.

[207] For example several 'celebrities', even MP's use this to prevent negative publication about certain private 'affairs', based on the UK 1998 Human Rights Act. Most relevant was so called Trafigura case in 2009, which forbade discussion or allegations the company had dumped toxic waste in Ivory Coast. See also: <http://skepticlawyer.com.au/2011/06/02/super-injunctions-privacy-and-twitter/> about the fading effectivity of this instrument in the light of new technologies (Twitter) cit: 6-13-2011.

'Among the checks and balances that a liberal society sets in place to curtail governmental domination and tyranny are strict limits on incursions into the private lives of citizens.'[208]

I am not that sure about the strictness of those limits; they are set by the relevant authorities, which will be considered in the following sections.

3.6 Derogations in a Public Emergency

The Principles make no clear distinction between threats to national and international security and so-called 'public emergency'. This public emergency might not be declared formally by law, but even so, this is an artificially constructed distinction between public emergency and threat of national security. Public emergency could be special circumstances in the sense of natural causes in the area of disasters as floods or health threats.[209] Also could be thought of environmental emergencies or other natural disasters. The question can be posed if all social unrest as a result of emergencies can be considered a reason for limiting fundamental rights as privacy. See the reference in par. 40 of the Covenant recognizing the difference but without defining it.[210]

When do internal conflict and unrest endanger the society or life of the nation? One cannot clearly distinguish the case of internal conflict threatening the life of the nation from more severe threats. It begs the question, as Stefan Sottiaux asks, in his thesis on Human Rights and Terrorism: to what extent can limitations on fundamental rights be justified in the name of protecting those very same rights and the democratic system as a whole?[211]

Economic difficulties per se cannot justify derogation measures.[212]

Still, the exceptional circumstances and threat of integrity are not defined. In the Siracusa Principles the determination of a certain legal status is not based on a particular analysis but reference is made to a situation that is considered to exist under those circumstances. Of course, this is a variable condition, dependent on the political system and policy within a certain state and is not always easy to determine based on a general rule that can be applied to all states, under all circumstances.

It is all about balancing the values of general interests with individual interests and human rights on the one hand, and balancing the general interest of protecting a society, in the name of international security and public safety, on the other. This balancing act reveals the

---

[208] H. Nissenbaum, *Privacy in context*, Stanford Law Books 2010, p. 92.

[209] The term Public Health Emergency of International Concern is defined in the IHR (2005) as "an extraordinary event which is determined, as provided in these Regulations:

- to constitute a public health risk to other States through the international spread of disease; and
- to potentially require a coordinated international response". This definition implies a situation that: is serious, unusual or unexpected; carries implications for public health beyond the affected State's national border; and may require immediate international action.World Health Organisation [who/int/ihr/procedures]

[210] 40. Internal conflict and unrest that do not constitute a grave and imminent threat to the life of the nation cannot justify derogations under Article 4.

[211] Sottiaux 2008.

potential for deducting a hierarchy of importance between the interest in protecting liberty from government interference and the interest in national security as a public good.

Circumstances are never clear though and in the case of international security or public safety the decision-making process is hardly ever transparent. In this respect, the role of governmental authorities, including the judiciary, is two sided: on the one hand they are concerned with the protection of those interests. On the other hand the authorities are concerned with justifying the incursion into individual rights for the sake of state security. Ideally, government should acknowledge that protecting privacy rights and security are not competing, but should be in balance and acceptable in a democratic society in accordance with an accepted legal framework.

A balancing system requires a certain degree of flexibility, but the fundamental character of the just balancing act also requires an important elementary basis of legal certainty. Natural persons should be aware by clear legal measures when and in what sense their fundamental rights can be 'postponed' or intruded upon in the name of national security or public order.

In principle citizens have the right to know which reasons can limit the protection of their fundamental rights from the perspective of legal certainty. The balancing of rights by governments has to be more transparent and based on categorical approaches rather than incidental approaches. The interpretation of rules, certainly in abnormal emergency situations, asks for flexibility, because, as Scholten states, there is never an absolute right that can be upheld under all circumstances. The balancing test will be considered less important if there is a threat that has devastating effects for the continuity of the nation, e.g. acts of destruction, terrorism and certain cyber-attacks.[213]

The danger of striving for absolute rights was recognised in discussions of freedom of the press in the First Amendment of the American Constitution in 1927.[214] In a time of perceived danger from communist infiltration, absolutism is considered to be dangerous: absolute rules would inevitably lead to absolute exceptions, and such exceptions would eventually corrode the rules.[215] Already in 1927 this danger is recognized:

''[The purpose of the speech-press clauses] has evidently been to protect parties in the free publication of matters of public concern, to secure their right to a free discussion of public events and public measures, and to enable every citizen at any time to bring the government and any person in authority to the bar of public opinion by any just criticism upon their conduct in the exercise of the authority which the people have conferred upon them. . . . The evils to be prevented were not the censorship of the press merely, but any action of the government by means of which it might prevent such free and general discussion of public

[213] The question, of course, is if the balancing is always visible if other regulations provide for the opportunity toderogate from the protection of fundamental rights as stated in the law for specific purposes. For instance, theretention regulations state that personal data as telecommunication traffic data may be used for criminalinvestigations as is described later in this thesis. Council Directive (EC) 2006/24 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 [2006] OJ L 105/54 (Data Retention Directive).

[214] Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

[215] Supreme Court (United States) June 4th, 1951, *Dennis v. United States* [1951], 341 US 494, 524; Sottiaux 2008, p. 29.

matters as seems absolutely essential to prepare the people for an intelligent exercise of their rights as citizens. '[216]

This opinion and the 'Dennis case' exemplify the challenge of balancing. The act of balancing is influenced by the state of political mind at a certain time and place. The American evolution of this concept cannot be ignored, although the primary focus of this thesis is on the European developments, in particular European Convention of Human Rights. This set of Principles concerning just use of derogation from the fundamental rights is a further specification of Article 29 (2) of the Universal Declaration of Human Rights that sets out the ultimate purpose of law:

In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

These provisions apply with full force to claims that a situation constitutes a threat to the life of a nation and hence enables authorities to derogate from non absolute fundamental rights as stated in the Covenant. How those provisions will be determined and on what laws these limitations will be based, concerning the limitation of the personal life, personal data and individual autonomy of communication is up to the room that is left for the sovereign states only to be limited by clear principles of law. Concentrating on Europe, the rulings of the European Court of Human Rights sheds light on these difficult questions.

3.7 European Convention on Human Rights and Decisions by the ECtHR on Public Interest

Article 8 of the European Convention on Human Rights (ECHR) defines the protection of privacy as a non-absolute fundamental right, providing for the limitation under the sixaforementioned circumstances as described in the Principles. Although there appears to be a legitimate guarantee on the limitation of these rights, it is not clear where these legal limitations lie. For example, Article 18 ECHR states:

'the restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed'. [217]

It is understandable that there are circumstances to allow the limitation of human rights if there is an important public interest that has to be protected by these measures. Nevertheless, these limitations are subject to an obscure legal balancing process to determine the applicable limitation. The Siracusa Principles, in spirit, are recognized in the interpretation of the limitation of fundamental rights of the Convention.

In the Convention, as in other international instruments of law and their national counterparts, there is a general reference to the limitation of rights.[218] However, a general restriction to the limitations is provided.

[216] Cooley 1927.
[217] McHarg 1999, p. 695.
[218] For example, Article 8(2)

Of course, the 'prescription' as stated in Article 18 can be rather broad. This prescription applies to the four fundamental rights, found in articles 8-11 of the ECHR, concerning privacy, freedom of thought, expression, and assembly and association. The possibility of limiting these rights is of a general character. The reasons for limitations for these four fundamental rights are comparable. Therefore, I will give examples of these limitations and intrusions on the general freedoms as described in these articles for reasons of analogy with the limitation of privacy.

The primary aspect that justifies the invocation of limitations are the statements 'prescribed by law' or 'in accordance with the law', as referred to in section 3.5.1 concerning the Siracusa Principles.

Most clear and therefore famous is the case Sunday Times v. UK,[219] concerning the freedom of expression. Although the subject is freedom of expression, the reasoning is even so applicable on the limitation grounds for privacy.

In this case reference was made to a (distasteful) settlement between Distillers Company (Biochemicals) Limited ('Distillers') that manufactured and marketed sedatives for, in particular, expectant mothers. In 1961 a number of women who had taken the drugs during pregnancy gave birth to children suffering with severe deformities. Reports concerning the deformed children had appeared regularly in The Sunday Times since 1967, and in 1968 the Times was critical of the settlement that was concluded that the same year. There had also been comment on the children's circumstances in other newspapers and on television. In particular, in December 1971, the Daily Mail published an article which prompted complaints from parents who feared it might jeopardise the settlement negotiations at hand. The Daily Mail was 'told off by the Attorney-General in a formal letter which threatened sanctions under the law of contempt of court, but contempt proceedings were not actually instigated.

On 24 September 1972, The Sunday Times carried an Article entitled 'Our Thalidomide Children: A Cause for National Shame'. This examined the settlement proposals then under consideration, describing the settlements as 'grotesquely out of proportion to the injuries suffered.' The article criticised various aspects of English law on the recovery and assessment of damages in personal injury cases and complained of the delay that had elapsed since the births. The article also appealed to Distillers Company Limited to make a more generous offer to the victims. In several instances injunctions were issued to the Sunday Times to withhold any publications on the subject and not influence the (new) negotiations between the parents and Distillers.

The main issue here, that is relevant for the discussion of privacy, are the bases invoked and determined as sufficient to restrict fundamental rights by the ECtHR.[220]

The Court examined whether the interference was 'prescribed by law', whether it had a legitimate aim cf. Article 10 (2) and whether it was 'necessary in a democratic society' for the aims of 'prevention of societal disturbances.

[219] ECtHR April 26, 1979, *Sunday Times v. UK* [1979], 2 EHRR 245.
[220] ECtHR April 26, 1979, *Sunday Times v. UK* [1979], 2 EHRR 245.

In this case, unwritten law in a 'common law country' is considered to comply with 'prescribed by law', as made clear in par. 47:

'47. (...) It would clearly be contrary to the intention of the drafters of the Convention to hold that a restriction imposed by virtue of the common law is not 'prescribed by law' on the sole ground that it is not enunciated in legislation: this would deprive a common-law State which is Party to the Convention of the protection of Article 10(2) (art. 10-2) and strike at the very roots of that State's legal system'.

Additionally, and importantly, law must be adequately accessible to citizens. This means that a citizen must understand under what circumstances what legal rules are applicable. So the access to and the comprehension of procedures and how the authority handles certain rules must be clear.[221]

The open-endedness of terms like 'pressing social need' and 'proportionate to the aim pursued' risk giving the state a broader 'margin of appreciation' of the terms on which limitations are considered acceptable.

3.8 Necessary in a Democratic Society

The laws, just as much as their exceptions, must be considered necessary in a democratic society as referred to in section 3.5.2 within the Siracusa Principles. The elements that can be distilled from the case law of the ECtHR are that intrusions are only to be accepted if the chosen means can be regarded as reasonable and suitable to achieve the legitimate aim, and consider the need to strike a fair balance between the demands of the general interest of the community and the requirements of the individual's fundamental rights.[222] In the 'Handyside case' the danger of what I refer to as 'exception creeping' is recognized by stating that there is no automatic, overwhelming importance given to the 'greater good' of protecting the interests of society as a whole. And this possible exception should always be applied proportionally to the perceived goal.

In the balancing act of both protecting the interests of society as a whole and of individuals, the overall aim of a democratic society must be explicated. The restrictions given in the second paragraph of for instance Article 10 (2) ECHR concerning the freedom of expression are not meant to fully restrict the freedom given in the first paragraph.[223] Although this case concerns another fundamental right the reasoning can be applied analogously to Article 8 concerning privacy.

---

[221] paragraph 79 states *Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*

[222] ECtHR September 23, 1982, *Sporrong and Lönnroth* [1982], A 52, s. 26, 28, par. 69, 73; ECtHR February 21, 1986, *James and others v UK* [1986], A 98, s. 35, 36, 37, par. 46, 51, 54, 56.

[223] ECtHR December 7, 1976, *Handyside v. UK* [1976], 1 EHRR 737, par. 137.

'The aim is to have a pluralistic, open and tolerant society. Of necessity this involves a delicate balance between the wishes of the individual and the utilitarian 'greater good of the majority'. But democratic societies approach the problem from the standpoint of the importance of the individual and the undesirability of restriction of the individual's freedom'. [224]

The balance between the fundamental right and the specific interest of society in the whole spectrum of different requirements that each entail, will create a pluralistic, open and tolerant society as a model of a democratic society. This can be considered as the next step of the concept of Habermas for making the people responsible for the society as a whole.

The concept of a democratic society does not preclude the possibility of States having legislation which protects other values, as in the *Handyside* case, the protection of the 'unspoiled mind of youth against moral deviance'. These national rules, though, must be tested against the meaning of the terminology used in the European Convention. For instance:

'*The reading of a prisoner's mail to and from a lawyer, ..., should only be permitted in exceptional circumstances when the authorities have reasonable cause to believe that the privilege is being abused in that the contents of the letter endangers prison security or the safety of others or are otherwise of a criminal nature.'*[225]

Therefore it must be clear that the 'fundamental right of mail secrecy' is misused and endangers security.

On top of that, the value of 'pluralism' is considered an undeniable aspect of democracy and is taken into account by the ruling of the court because the rule of law has to fit within the concept of democracy as such:

'*As the Court has said many times, there can be no democracy without pluralism'.*[226]

The law has to be aligned with democratic principles such as openness and tolerance. Furthermore, a democratic society has the obligation to make laws transparent and accessible for its nationals and anyone who will be subject to them. Moreover, in a democratic society, it is the duty of the government to defend its decisions which limit the rights of its citizens." To put it extremely, being the Goliath against David it should be the obligation of the governmental authorities to defend their decisions to limit the rights of the citizen. Otherwise, the outcome from this battle will be contrary to the Bible tale.

3.8.1 Burden of Proof

Although transparency of a decision to apply a limitation is a conditio sine qua non, sometimes the government believes justification for an intrusion is not needed because the state's subject (applicant) has to prove that the application of the intrusive rule is not

[224] Ibid [146/147].
[225] ECtHR March 25, 1992, *Campbell v. United Kingdom* [1992], A. 233. *(par.48)*
[226] ECtHR January 30, 1998, *United Communist Party of Turkey and others v. Turkey* [1998] 26 EHRR 121, par. 43.

acceptable.[227] This is the world upside down, the State has to defend that it has been a just measure

In the *Handyside* case, the Commission (ECsHR) avoids drawing limits to freedom of expression by instead granting that the state has a certain degree of discretion in determining the necessary limitations (of freedom of expression) in accordance with Article 10 (2). But this has to be scrutinized constantly by the national government to keep the democratic degree to society. Strangely the European Human Rights Commission is of the opinion that it is impossible to impose any uniform standard of morality on member states. It finds no violation of Article 10.[228]

In the *Handyside* case the challenge to the right of freedom of expression pertained to the prohibition of a book, on the basis of the Obscene Publication Acts of 1959 and 1964, entitled 'The little red schoolbook' with some guidance on sexual behaviour. Authorities deemed the book obscene and threatening to the public interest and seized it from the distributor.

The applicant stated that, in line with the jurisprudence of the Commission relating to the margin of appreciation, the burden was on the respondent Government. The European Commission of Human Rights was tasked with balancing the principles of the treaty as a ruler against the national regulations.[229]

Although the seizure and destruction of the schoolbook constituted a 'prima facie' interference with the peaceful enjoyment of possessions within the terms of Article 1 of protocol No 1,[230] this seizure on the basis of the national interest was permitted.

The dissenting opinions of judges Mosler and Zekia indicated that they were not convinced that this interference was justifiable.[231]

Intrusion of one's freedom of information or the personal sphere of communication considers intrusion on non-absolute, though fundamental rights and are allowed within the context of a democratic society. It may never go beyond the meaning of proportionality of the measure towards the purpose that is pursued that is as is made clear in the following paragraph.

3.8.2 Intrusion of Human Rights for Reasons of National Security, Proportionality

[227] ECtHR December 7, 1976, *Handyside v. UK* [1976], 1 EHRR 737.
[228] ECtHR December 7, 1976, *Handyside v. UK* [1976], 1 EHRR 737, par. 165-167.
[229] Art. 3 ECHR: *Every member of the Council of Europe must accept the principles of the Rule of Law and of the enjoyment by all persons within its jurisdiction of human rights and fundamental freedoms, and collaborate sincerely and effectively in the realisation of the aim of the Council as specified in Chapter I.*
[230] Article 1. Protection of Property: *Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.*
The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.
[231] Diss. Opinion judge Mosler: I am not convinced that the measures taken by the British authorities, including the judgment of the Inner London Quarter Sessions, were 'necessary', within the meaning of Article 10 par. 2 (art. 10-2), for the achievement of their aim, namely the protection of morals.(…)

As a clear example of the intrusion into human rights to defend national security interests, I will refer to the most far-reaching intrusion on human rights, namely the intrusion on human life.

In this case, a former (volunteer) GDR border guard (Grenztruppen der DDR) was a member of the National People's Army (Nationale Volksarmee) of the German Democratic Republic. This person was alleged to have killed an unarmed fugitive. The alleged GDR border guard claimed that he had (merely) followed the orders of the national authorities at that moment.

Although the justification of 'necessary in a democratic society' that has become familiar, it is clearly not straightforwardly applicable to intrusions on the human life.

Of course, the concept of 'necessary in a democratic society' was interpreted in a way that would not be acceptable in Germany of today, but has to be placed in the context of the German Democratic Republic of that time.

The Federal Court of Justice observed that a justification which placed the prohibition of crossing the border above the right to life

'flagrantly and intolerably infringe[d] elementary precepts of justice and human rights protected under international law'[232]

and was invalid. It also referred to a severe infringement of the Universal Declaration of Human Rights.[233]

Moreover, the Federal Court of Justice stated that the decisive factor was that the killing of an unarmed fugitive by sustained fire was, such a dreadful act, not justifiable by any defence whatsoever, that it must have been immediately apparent and obvious even to an indoctrinated person that it breached the proportionality principle and the elementary prohibition on the taking of human life. This example is a clear intrusion of the integrity of the personal sphere of a human being. One could expect such difficulties with determining the primary purpose of surveillance drones which have the dubious role in (in)directly inflicting physical harm.
Although the taking of life is not the primary purpose, one never knows to what extent the use of 'drones' in surveillance will be applied in inflicting physical damage.[234]

Even in a democratic state like the Netherlands, national (security) interests can overrule all democratic principles. A clear justification can be found in Article 68 of the Netherlands Constitution:

Ministers and State Secretaries shall provide, orally or in writing, the Houses either separately or in joint session with any information requested by one or more members, provided that the provision of such information does not conflict with the interests of the State.

---

[232] 'Verstösst offensichtlich und unerträglich gegen elementare Gebote der Gerechtigkeit und gegen völkerrechtlich geschützte Menschenrechte'.
[233] ECtHR March 22, 2001, *K.-H.W. v. Germany* [2001], App. No. 37201/97, 36 EHRR 59.
[234] Although this is no question anymore concerning the use of drones in 'war areas' as Pakistan and Afghanistan

Essentially, the government of The Netherlands may, under the Constitution, limit access to information on the part of the Parliament and the Senate. So the ultimate institution of a democratic country of The Netherlands, Parliament and Senate will be kept out of information by the government if this government decides to do so. Interesting to see is the vision on this aspect of 'democracy' of a Dutch Senator concerning the new law on information and security agencies:

People expect as the primary task of governments, the bearing of the sword, protection of the people against threats and terror. Therefore, even the European Court of Human Rights leaves ample competence to the national authorities to interpret public order and national security as national intelligence agencies see fit'.[235]

This observation is contested, nowadays, by the publications of the 'Snowden papers' in the Guardian. National authorities, national authorities, often under the guise of their respective intelligence agencies, have a wide-reaching understanding of 'in the interests of national security.[236]
The right to an undisturbed life for citizens is touching on the integrity of body and mind. It is a severe intrusion if authorities, for the sake of common good are using their power to limit those rights without a well balancing of all interests.
In the next Chapters a selected set of regulations and case law will be scrutinized on having a credible and proportional basis in the law to limit the protection of the personal sphere of natural persons for reasons of public order and security with special reference to anti-money laundering and related anti-terroristic regulations.

3.9 Concluding Remarks on General Limitations on Fundamental Rights

In this chapter I sought to answer two questions:
How does the (inter)national legal framework on human rights allow for governments to limit privacy?
What principles should govern the exceptions to privacy in this respect?

We have seen a great deal of flexibility in the applicability of the right to privacy. We see that the open norms in limitation give opportunity to a rather broad interpretation of limitation grounds. In general, the right to privacy tends to be limited by at least one of the following three legal instruments.There is a triple limitation opportunity; first the international legal instrument, ECHR or ICCPR gives a general limitation ground, then the national laws based upon these treaties state the limitation grounds and thirdly, e.g. on grounds of the national

[235] '*What people expect of authorities is the primal task, the sword worn by government to protect them and theirs against terror*' ('Wat mensen van overheden verwachten, is in zekere zin de oertaak, het zwaard dat de overheid draagt: bescherming van hen en de hunnen tegen onder andere terreur', Senator Döll, lid Eerste Kamer Inlichtingen- en veiligheidsdiensten. binnentreden woningen 5 februari [] Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de Inlichtingen- en veiligheidsdiensten 19[..]) (25877) <http://parlis.nl/pdf/handelingen/HAN7374A03.pdf>.
[236] In the Sunday Times v. The United Kingdom (No. 2) and the Observer and Guardian v. The United temporary injunctions were imposed in relation to the book 'Spycatcher', the memoirs of Mr. Peter Wright, a retired member of the British security service living in Australia. The book includes an account of allegedly illegal activities by that service. In September 1985 the Attorney General of England and Wales instituted proceedings in Australia on behalf of the United Kingdom Government to restrain publication of the memoirs. They were eventually published there in October 1987, after the Court of Appeal of New South Wales had given judgment in favour of the author and his publishers. ECtHR November 26, 1991, *The Sunday Times v. The United Kingdom (No. 2)* [1991], A 217, App. No. 13166/87.

security interests and overarching political interests of the time the national policy will apply and adjust the rule. All three grounds are scrutinized by either national courts or the ECtHR. We find that within the specification of the norms in the human rights area, applicable to the limitation of privacy, courts apply the principles which we also find in the Siracusa Covenant. Within the limitations boundaries are set as mentioned in paragraph 3.4.1

- The limitation must not be interpreted so as to jeopardise the essence of the right concerned; strictly in the light and context of the particular right; prescribed by law and be compatible with the object and purpose of the legal instrument, i.e. the essence of the regulation that is to be used to apply the limitation; based on a law which describe specific circumstances that allow the limitation; there must be a pressing social need, assessed on a case-by-case basis, justified by the protection of a strictly limited set of well-defined public interests.

The Siracusa Principles give an overview of the possible reasons that are accepted in national and international law to limit the contents and the practical adherence to fundamental rights. These principles are intended to be applied to all limitations of non-absolute fundamental rights. The application of the Principles is already taking place if we look at several rulings of national and international courts. The problem is the actual use of the Principles within the balancing of interests. The factors used to weigh the applicability of the principles are not always entirely clear and justified.
Certainly, the 'general interest' of national security is weighed against the individual fundamental right of privacy and freedom of expression. To fight (cyber) terrorism, acceptable measures within a democratic society are often stretched in a dubious way, as can be seen in the exchange of vast amounts of personal data between befriended intelligence agencies without specification of purpose. It may also be that the origin of this information can be obtained by non 'democratic' activities'.[237] This is a worrying development in individual cases but even in balancing between the protection of fundamental rights as a legal obligation of authorities, and the general interest of security, the former interest often succumbs. This can be seen in familiar, everyday examples like the disproportionate security controls on airports, the declaration of so called 'security areas' in the centre of Amsterdam where surveillance and even physical searches by the police are permitted without court order and as other example in The Netherlands, the permanent control and storage of photographed license plates to be used in case of possible police investigations or cases of national security. More of the case law on the exceptions to privacy, will be discussed in the next chapter.

[237] In The Netherlands there were parliamentary questions about the use of digital ether information received by satellite dishes in Burum by The Netherlands Sigint organisatie (NSO) that was made available to the NSA. NSA took military action on basis of this info using 'drones' that made human victims. Another cynical example is in the report of the Supervising Committee on The Netherlands Intelligence Services where the observation was made that 'the origen of the received information of befriended services could not be analysed in such a way that made clear if the information was obtained by torture' p. 86/87 CTIVD rapport nr. 38, 2014

4 The Applications of the Exceptions in ECtHR Case Law, specifically on Article 8(2)

4.1 Introduction to the Limitation Actions

In Chapter 2 privacy is described as a sphere of personal integrity the protection of personal integrity from intrusion from the outside world. Many scholars have repeated each other or added elements or further specifications to a legal definition, or at least a conception, of the term privacy. Connected to this research, which is considering the role of government in limiting the citizen's fundamental right, the essence of the concept of privacy is non-intrusion and individual autonomy concerning any elemental information relating to a natural person. In short, the inviolability of a natural person's personal sphere in a broad sense. In the information age the boundaries of the concept of privacy in a theoretical sense still exist, but the means to intrude upon privacy have changed and increased in intensity. The technological means have expanded and are used in all segments of society by natural persons and legal persons in different capacities.

Electronic networks mould the values and boundaries of privacy. The distinction between public and private information tends to get blurred. Governments are using public and private information and are intruding upon the private sphere of individuals and other governments. As such, the legal instruments that limit the fundamental right of privacy must be specified meticulously. The problem is that the understanding of the intrinsic value as well as the perception of what is considered 'privacy sphere' is continuously changing. Governments adapt their investigative instruments to these developments, using more and more data of their citizens to fight criminal behaviour, protect security and protect the 'democratic' order.

The question to be answered in this chapter is:

> How does the European Court of Human Rights validate, in its case law, exceptions to privacy? On which principles are the decisions based?

In the following chapters I select a range of binding legal instruments of national and international law, in which limitations of privacy are encompassed. These regulations, in increasing specification are: general human rights agreements, privacy agreements, and information society specified regulations in the telecommunications and financial sectors. All of those regulations are increasingly influenced by the developments of the information society. The tendency of (international) governments has been to respond to the electronification of the world with calls for greater surveillance, using increasingly intrusive techniques, to control societies.

Within the articles in treaties, covenants, regulations and directives in the areas enumerated hereunder, the limitation of privacy by means of special provisions are compared and used to illustrate the problems that exist in the use of those limitation provisions. Finally, I will show that many of the (unintended) (mis)uses or misinterpretations of the limitations follow from inconsistencies in terminology. This can be observed in the decisions by international legal courts, mainly supported by (European Court of Human Rights) case law.
In general, the limitation of a human right is exercised by state authorities on the basis of their sovereignty. This aspect of statehood is vulnerable and the limitation of sovereignty is only

accepted under very high political, economic or military pressure. In the first draft of the Universal Declaration of Human Rights there was the general limitation clause in Article 29 par. 2, being one of the main requirements to accept the set of fundamental rights by the participating parties:

> *'In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.'*[238]

The general limitation clause was included in the Recommendation adopted by the Consultative Assembly on September 8, 1949 as well as in one of the alternative drafts proposed to the Committee of Ministers by the Committee of Experts on March 16, 1950.[239]

4.2 Differentiation of Crimes against National Security and Prevention of Crime in General

Although there are more reasons to limit privacy, the focus in this thesis is on the security and crime fighting area.
The limitation of privacy is based on reasons of preventing crime and protecting national security. In general, national and international security rank higher than public order and protection against criminal acts in terms of the (perceived) threat and damaging consequences to society. Therefore the (perceived) actions, which are thought to threaten national and international security, will touch upon 'exceptional circumstances' giving the possibility for authorities to use more severe legal measures. Limitations of privacy on security grounds are less controlled by democratic institutions, such as parliaments, by virtue of the 'secret' nature of these measures. The nature of intrusions into fundamental rights should ask for more intrinsic guarantees as specification of measures and circumstances as well as independent control on the actual execution of the limitations. Intrusions embedded in criminal laws are less vague and know more safeguards than those in security law. Moreover, the competence of authorities and justifications for applying intrusive investigative powers differ. Police investigative activities such as tapping, placing tracking devices, or conducting computer searches, are always based on a court order. National security in, for example, The Netherlands does not require such an additional guarantee. Just a general mandate of the minister of interior or the director of the Service is sufficient

This view is supported by Cameron, who draws this conclusion in support of the use of Article 8 ECHR concerning national security.[240] Decisions to limit one's right to the protection of personal life and personal information, including the protection of personal data for reasons to protect the public order, have more guarantees in material law and the procedures based on

[238] See Christoffersen 1990, p. 72 § 40 and p. 74 § 57-62, on p. 80, note 458 and note 461: The Teitgen Report of September 5, 1949 comprised the following limitation clause: 'In the exercise of these rights, and in the enjoyment of the freedoms guaranteed, no limitation shall be imposed except those established by the law, with the sole object of ensuring the recognition and respect for the rights and freedoms of others, or with the purpose of satisfying the just requirements of public morality, order and security in a democratic society.'
[239] Referring to 461 Council of Europe: 1 Collected Edition of the 'Travaux Préparatoires' (1961) p. 105. See Chapter 1.1.1, Idem note 4, p. 80.
[240] Cameron, 2000

formal criminal law than security law based actions by NSA's.[241] From national and international perspectives, found in court decisions as well as in international fora and scholarly publications, the discussions about the differences between protecting security and fighting crime prove that there is not always a clear distinction between the two objectives.

4.2.1 Interpretation: Terrorism vs. Ordinary Crime

In Article 3l of the Vienna Convention on the interpretation of treaties, it is stated that a treaty shall be interpreted in good faith, in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.[242] A clear example of problems with that principle can be found in the Golder case before the European Commission of Human Rights. The Golder case concerned the seizure of letters of the prisoner Golder in light of preventing criminal acts and protecting state security. Judge Fitzmaurice in a separate opinion offers this peculiar reasoning concerning the limitation of privacy:

'There shall be no interference by a public authority with the exercise of this 'right' if the correspondence itself is not allowed'.[243]

This is puzzling given there is no fundamental right to send letters on the part of the prisoner. In addition.
The other interesting aspect in this case is the point of classifying the act of letter-writing/ exchange as a criminal offence. Depending on the purpose and circumstances, sometimes a certain 'crime' or criminalized behaviour, which is content-wise exactly the same, may be perceived as a threat to national security, a terrorist action or simply damaging to property.

The separate opinion of judge Fitzmaurice sheds some light on the 'fusion' of two classifications of the same offence, explaining that within the context of the circumstances it is to be decided if a certain action is considered to be responding to a threat to security or to the prevention of crime. In this case both categories were applicable as, he explains, the categories can be considered different categories and – considering the circumstances – -can be decided upon in different law regimes, competences and different measures:

> *'control of a prisoner's correspondence is capable of coming under the heads both of 'public safety' and 'the prevention of disorder or crime', thus ranking as an excepted category whichever of the two above described methods of interpreting this provision might be adopted.'*

---

[241] See: Cameron 2000, p. 50.

[242] Vienna Convention on the law of treaties
Vienna 23 May 1969; : Article 31 General Rule of Interpretation
1. *A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose*.(…)

[243] See the elaboration of Judge Fitzmaurice in the 'Golder' case: '*There shall be no interference by a public authority with the exercise of this right', which appears at the beginning of the second paragraph of the Article (art. 8-2), - the right itself being stated in the first paragraph (art. 8-1) to be the right of the individual to 'respect for his private and family life, his home and his correspondence'. It would be easy to close the argument at once by saying that correspondence is not 'respected' if it is not allowed to take place at all. But the matter is not so simple as that. It could undoubtedly be contended that correspondence is respected so long as there is no physical interference with whatever correspondence there is, but that the words used neither convey nor imply any guarantee that there will be any correspondence; so that, for instance, a total prohibition of correspondence would not amount to an interference with the right.*

So interpreting articles of a treaty in their context, and in the light of the treaty's object and purpose, can lead to different interpretations in the same case, making the balancing of good faith not a very consistent measure for action.

An example of defining acts on the basis of their context can also be found in the EU framework decision, which states that acts,[244]

> '*which, given their nature or context, may seriously damage a country or an international organisation' should be regarded as an objective requirement for qualifying punishable behaviour as a terrorist offence. (…) to pose a certain threat of politically or publicly motivated violence. (…) If no damage was caused and no threat of damage existed in a specific case, the qualification 'terrorist offence' would not apply. This establishes a clear distinction between terrorist and non-terrorist varieties of the punishable behaviour referred to in Article 1(1)*[245]

The limitation of the protection of the fundamental right of the concerned subjects based on the intent of the perpetrator should be described in the applicable law. A terrorist act as such, as defined in Article 83 of the Dutch Criminal Code, can entail numerous crimes if the actions are perpetrated with 'a terroristic intention'. Interpretation of this intention is essential to how an act is classified and is often based on circumstantial evidence, culture, (religious) background and individual contacts. These variables make the balancing act of 'good faith' difficult and inherently inconsistent.
In the phase of investigation and surveillance, the police as an investigative authority needs a court order to permit the use of intrusive means that breach the personal sphere, for example camera's, GPS tracers and computer/data. Most national security agencies are allowed to use the same intrusive means without any legal control except for the permission of the director of the agency. This results in a devaluation of legal control because this information, gathered by national security, certainly will be handed over to the police if a terroristic crime is suspected by a certain person.

4.3 Crime and National Security

Article 8(2) ECHR requires that there is a basis in the law and a necessity for the democratic society to limit the rights mentioned in Article 8.1. It is not clear whether there is a difference of guarantees and limitations on the protection of privacy, based on the competences of different agencies, i.e. police/justice and national security agencies. It is all the more unclear when both the police and national security agencies are involved in the same case. The question arising from this dichotomy is whether it is possible to define a certain (quality) control on the use of this limitation by international organisations such as the EU and by national states in their different regulations. It will be a sensitive process because it often concerns state security issues under various, unique circumstances.

Additionally, sovereign states differ in their opinions of whether a certain crime can be considered as endangering national security and therefore may be defined as a terroristic activity or 'just' as a criminal act. Again, such a determination is often set by considering the intent of the act and its outcome.

[244] COM (2001) 521 final.
[245] Borgers 2012.

It remains unclear however to what extent the outcome of the act, namely endangering society, meets the criteria of a terrorist act and consequently, to what extent the fundamental right to privacy may be limited and by whom.[246]

Restrictions on fundamental rights require a weighing process between the general interest to protect the security of society, on the one hand, and the importance of protecting the fundamental right of the individual citizen, on the other. The obligation to protect fundamental rights as a general obligation of the state is, regrettably, often overlooked in this balancing process)[247]

Although these balancing processes are normally found in the area of public and national security (mainly counterterrorism), they are also found in the field of access to public information (WOB)[248]in European case law.[249] These considerations are dependent upon the seriousness of the threat to society or upon the relevance of the protection of the considered rights of the concerned subjects.

In the following I will refer to the most important European case law in this respect of balancing security against privacy.

In this 'weighing process' some of the aspects are very notable in their relevance to society. Dangers to national security are considered more disrupting to society than 'normal' criminal activities and therefore allow for more extensive limitations on fundamental rights. This certainly applies to the national security agencies, based on umbrella like articles within national security laws. The risk of crossing the borders has been considered as a justification for the acceptable use of intrusive instruments

> *'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'*[250]

The *Malone* v *UK* case before the ECtHR determined that no right guaranteed by the European Convention should be interfered with unless a citizen knows the basis for the interference through an ascertainable national law.[251] In Kruslin v. France,[252] concerning the use of surveillance techniques, it was stated by the European Court that:

---

[246] Borgers 2012, p. 68.

[247] . Golders & Williams present this aspect: *From our analysis of international, regional and domestic human rights instruments, we conclude that human rights, whilst central to the operation of modern western liberal democracies, are nevertheless not inviolable.That is, they can be abrogated or modified in the pursuit of countervailing or overriding societal objectives, such as the protection of national security. We thus argue that the proper method for assessing the new counter-terrorism laws, from a human rights perspective, is to adopt a ''balancing approach'' according to which the importance of the relevant human right is weighed against the importance of the societal or community interest in deciding whether to take legislative action (or, from the position of a judge, in deciding whether a certain law is valid* . Golder & Williams 2006, p. 45.

[248] The Dutch Freedom of Information Act

[249] Joined Cases C-92/09 and C-93/09, *Schecke en Hartmut* [2010] ECR I-11063. Case C-28/08, *Commission/Bavarian Lager* [2010] ECR I-06055.

[250] See e.g. ECtHR December 4, 2008, *S.* and *Marper v. the United Kingdom*, §112.

[251] ECtHR August 2, 1984, *Malone v UK* [1984], 7 EHRR 14; ECtHR March 26, 1987, *Leander v Sweden* [1987], 9 EHRR 433.

[252] ECtHR April 24, 1990, *Kruslin v. France*, 12 EHRR 546.

'It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated'.

And in the case *S. and Marper v. the United Kingdom*:[253]

'The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned....'

Concerning the interception of communications, the Court stated that this represents a 'serious interference' with private life, therefore the law must be particularly precise.[254] With regard to interferences with private life in the 'prevention of crime' context, it appears that the European Court is demanding increasingly rigorous legal provisions as made clear in the case *Valenzuela v. Spain*,[255] which is further discussed in section 4.4.3.

The necessity to have (clear) regulations governing the use of electronic surveillance devices is clarified in the case of Malone v Metropolitan Police Commissioner No.2.[256] Malone was prosecuted for handling stolen property and during the trial it became apparent his phone was tapped. Malone contested the legality of the interception, but it was not forbidden to do so by law because it was allowed under 'home office guidelines'. The ECHR decided that his right to respect for private life under Article 8 had been infringed. The act of interception of a telephone call in essence infringed upon both 'private life' and 'correspondence', both protected in Article 8(1). The law must thus be adequately accessible and foreseeable; that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and in the manner of its exercise.[257] The Court acknowledged that although Home Office guidelines governed the use of the telephone tap, this did not satisfy the requirement that an infringement of a person's right to respect for their private life could be legitimised if there was 'a legal rule directed towards one of the legitimate exceptions. Quality, clarity and transparency are also of the utmost importance to credible limitations to privacy within the law in a democratic society. Still, on the basis of case law, it is accepted that espionage, subversion and support of incitement to, as well as terrorist activities itself, are considered as disrupting to society and disturbing to the public order. These acts also are found under national security issues.[258] The case law reveals a tendency to weigh more heavily the general interest of society (in the case of national security) over the individual fundamental right to privacy.
In the Klass case, five lawyers contested the fact that subjects were surveyed by the German State authorities. The contesters were claiming that Article 10 par. 2 of the Basic Law

[253] Case of S. and Marper v. the United Kingdom, Application no. 30562/04 and 30566/04 §99, §103.
[254] ECtHR March 25, 1998, *Kopp v. Switzerland* [1998], 27 EHRR 91.
[255] ECtHR July 30, 1998, *Valenzuela Contreras v. Spain* [1998], 28 EHRR 483.
[256] ECtHR, *Malone v. Metropolitan Police Commissioner* No.2 [1979], 2 WLR 700; subsequent; ECtHR August 2, 1984, *Malone v. UK* [1984], 7 EHRR 14.
[257] See *Malone v. the United Kingdom,* August 2, 1984, §§ 66-68, Series A no. 82. Further, 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. Rather, the law must be sufficiently clear in its terms so as to give citizens an adequate indication as to the circumstances in which and the conditions on which the [police] are empowered to resort to this secret and potentially dangerous [measure]. (Malone v. UK: para. 67).
[258] ECtHR September 6, 1978, *Klass and others v. Federal Republic of Germany* [1978], 2 EHRR 214.

(Grundgesetz) and a statute enacted in pursuance of that provision (G10),[259] were contrary to the ECHR because the subjects were not informed about the surveillance measures that were used afterwards. The Court held unanimously that it was necessary to regard the applicants as possible victims in the special circumstances of the case but that the measures taken, having regard to the safeguards provided, although interfering with the right guaranteed in Article 8(1), were 'necessary in a democratic society in the interests of national security' within the terms of paragraph 2 of Article 8.[260] In this case it is clear that on the basis of this limitation, all kinds of intrusions by authorities on the personal life are considered legal under different circumstances.

The principle, 'necessary in a democratic society' as presented in article 8(2) ECHR and specified in the Siracusa Principles, were arguably overstretched in the Klass case:

> *The cardinal issue arising under Article 8 in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article. This paragraph, (...), is to be narrowly interpreted. 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.*[261]

Of course, the most relevant (cardinal) question is what type of surveillance is accepted within the context of the case and democratic society in general. How intrusive a surveillance instrument may be used depends on the circumstances of the case, the endangerment of society and applicability of the subsidiarity principle. All of this, in turn, should be considered against the background of the state of the art in technology and the (perceived) threat and political footprint of the society itself. For instance, on February 2013, an increasing limitation of the fundamental and democratic rights was taking place in Russia concerning the right on demonstration, right on freedom of speech and protection of privacy. Based on the Klass decision, a narrow interpretation of the Convention would be enough ground (in case of complaints) not to accept the limitation of these rights, even if they are based on law (in which for instance (illegal) demonstrations are to be punished by a 100 fold increase of fines).[262]

In establishing the degree of intrusion into one's personal sphere, I refer to the set of intrusive actions described by Cameron. Cameron discerns several ways of intrusion by ways of (secret) directed surveillance entailing the gathering of data of individuals (by physical and electronic means). [263] He excludes monitoring society, but it should be included if it refers to special activities relevant under Article 8(2) ECHR. Cameron's extensive list includes: the interception of letters and parcels; (concealed) electronic camera surveillance; microphone and recording surveillance; conversation recording over public or private telephone lines; metering information and location information; information from the use of identity cards and identifying elements as fingerprints, retina; and finally, collating information from all kind of databanks and data collection, i.e. social security and financial institutions. Although rather complete, Cameron wrote this list in the year 2000 and it bears updating, to include: the use of

[259] Namely the Act of August 13, 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications
(Gesetz zur Beschränkung des Brief-, Post- under Fernmeldegeheimnisses, herein after referred to as 'the G 10').
[260] Ibid [48].
[261] Ibid [42].
[262] As was the case in Russia in February 2013.
[263] Cameron mentions nine different ways but several distinctions can be combined and mentioned as one, p. 77.

advanced data mining in public information and social networks and the use of Wi-Fi, RFID, blue-tooth by smart phones, tablets or other means.

The use of information from the public domain may also entail an intrusion on private life. In the case *P.G. and J.H. v. the United Kingdom*, the Court considered that the recording of data and the systematic or permanent nature of the record could give rise to private-life considerations even though the data in question may have been available in the public domain or otherwise. The Court noted that a permanent record of a person's voice for further analysis was of direct relevance to identifying that person when considered in conjunction with other personal data. It accordingly regarded the recording of the applicants' voices for such further analysis as amounting to interference with their right to respect for their private lives.[264]
The seizure of data and surveillance activities are separated by Cameron, discerned as of a different legal orders. Although this may be applicable to physical elements of information such as the seizure of paper, computers and other physical objects, it is not clearly the case with the electronic form. It is conceivable that some could argue that the seizure of data never can take place because it is not tangible. But personal data also are essential to the personal life that can be endangered or its value diminished by the intrusion or by its seizure.

4.4 ECtHR Case Law on Restrictions: Balancing the Process

Restrictions on the intrusion into the right to privacy can only be acceptable if the boundaries are clear. There is a great deal of ambiguity conflating the general misbehaviour of individuals in a criminal sense with individuals endangering national security, within an accepted legal framework, which can result in the use or intrusion of information of a personal character. Abuse of these possibilities of authorities to limit privacy in the sense of 'detournement de pouvoir' by a state/authority will never be acceptable, even under endangering circumstances. The Vienna Convention says as much, setting the standard. One question remains: how do States invoke the 'good faith' principle of interpretation to justify the use of intrusive technologies? [265]

The restriction will only be applicable in the case of non-absolute rights, for example the right to the protection of the private life.

Concerning the limitation of the elements of the fundamental right on privacy on basis of Article 8(2) there are three main requirements that have to be fulfilled to legitimize the intrusion, at least to make this acceptable for international law. The intrusion has to be based on law and must be necessary and acceptable in a democratic society. The additional requirements include: the purpose of the intrusion must be valid; the protection of the national security must be at stake; public safety or the economic well-being of the country must be at stake; intrusions are for the sake of the prevention of disorder or crime or for the protection of health, morals or for the protection of the rights and freedoms of others. The proportionality of the measures are to be weighed on a case by case basis, entailing legal and often political review.

[264] See *P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§ 59-60, ECtHR 2001-IX as also referred to in *S. Marper v. UK*.

4.4.1 Limitation in an Emergency or Normal Situation?

It can be difficult to discern the normal situation from the emergency situation. Consequently, the application of limitation rules can be tenuous. Concerning security issues, Cameron studied the application of limitations in relatively 'soft' emergency situations.[266] This can also apply to (semi) normal situations. But what is a normal situation in a 'risk'-based society? Cameron's orientation relates to (almost) normal, relatively peaceful situations. This qualification will apply to almost any period, place and political climate. As such, it applies to the regulations that relate to the detection and prevention of terrorist and terrorist-supporting activities as for instance anti-money laundering legislation.

Most studies concerning the limitation of fundamental rights are orientated toward 'real emergency' situations and the limitations possible under Article 15 of the European Convention on Human Rights.[267] Article 15 enables all but the absolute rights in the Convention to be suspended in 'time of war or other public emergency threatening the life of the nation' provided this is 'strictly required by the exigencies of the situation'. The specifics of the situation though are not made clear and depend on interpretation of the authorities and the use of the law system that is applicable under those circumstances.[268] The existence of the 'public emergency' should be proved by the state derogating from its obligations be it that:

'*[b]y reason of their direct and continuous contact with the pressing needs of the moment, the national authorities are in principle in a better position than the international judge to decide both on the presence of such an emergency and on the nature and scope of derogations necessary to avert it*.

In this matter, Article 15(1) leaves the authorities a wide margin of appreciation.[269] Threats by terrorist action, certainly after 9/11, are conceived of as public emergencies.[270] In this case, the UK has sent a derogation notice to the secretary General of the Council of Europe which was justified as follows:

There exists a terrorist threat to the United Kingdom from persons suspected of involvement in international terrorism. In particular, there are foreign nationals present in the United Kingdom who are suspected of being concerned in the commission, preparation or instigation of acts of international terrorism, of being members of organisations or groups which are so concerned or of having links with members of such organisations or groups, and who are a threat to the national security of the United Kingdom.

On the basis of this notice, the Anti-terrorism, the UK Crime and Security Act 2001 was adapted to arrest and detain any foreign national who was considered to be a threat. 11 people with different nationalities were arrested and detained for several years. In this case the ECtHR

---

[266] Cameron 2000, p. 9.

[267] '*In time of war or other public emergency threatening the life of the nation, any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.'* See also Agamben 2005, p. 57.

[268] Greer 1997, p. 5.

[269] Ireland v United Kingdom (1978) Series A No 35 at 78–9, refered to by Tahmina Karikova, *Derogation from human rights treaties in situations of emergency*, http://bit.ly/1yw56TD

[270] *A and Others v. United Kingdom*, Application no. 3455/05, Council of Europe: European Court of Human Rights, 19 February 2009

ruled: *'that that only a narrow interpretation of these exceptions is compatible with the aims of Article 5*(right to liberty and security).[271]
But still, the 'narrow interpretation' did not stand in the way of intrusive measures to persons that form a threat to society. And who could judge that situation better than the national authorities and courts?

Additionally,

'*As previously stated, the national authorities enjoy a wide margin of appreciation under Article 15 in assessing whether the life of their nation is threatened by a public emergency. While it is striking that the United Kingdom was the only Convention State to have lodged a derogation in response to the danger from al-Qaeda, although other States were also the subject of threats, the Court accepts that it was for each Government, as the guardian of their own people's safety, to make their own assessment on the basis of the facts known to them. Weight must, therefore, attach to the judgment of the United Kingdom's executive and Parliament on this question. In addition, significant weight must be accorded to the views of the national courts, which were better placed to assess the evidence relating to the existence of an emergency*.[272]

The Court ruled that the actions in general were justified. But limitation of the rights of subjects also, even more often, takes place under 'normal' circumstances, be it to prevent criminal behaviour or to protect the security of the state. Notwithstanding the fact that public emergency is not very well-defined, it is even more vague under which circumstances, in a 'normal' situation, a threat to the national security and public order, or the prevention of crime, may suspend or limit privacy. Therefore, the European Court of Human Rights had to develop a more specific legal boundary for the limitation of fundamental rights under more 'normal' circumstances.[273] Dependent upon the necessity of those measures, the Court decided in several cases that 'security' and public order in 'relatively' normal situations ask for more guarantees and other motivations to apply limitations on the right of privacy than within emergency situations when Article 15 is applicable.[274]

For instance, in the 'Lawless' case[275] G.R. Lawless, a professed IRA member, was detained without trial and claimed that the Convention had been violated by the authorities of the Republic of Ireland. Nevertheless, the Irish law stated that
'*A member of an unlawful organisation in contravention of this section shall be guilty of an offence,'*[276]

---

[271] *A and Others v. United Kingdom*, Application no. 3455/05, Council of Europe: European Court of Human Rights, 19 February 2009, para 171
[272] Idem, para. 180
[273] ECtHR July 1, 1961, *Lawless v. Ireland* [1961], 1 EHRR 15.
[274] '(1) In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.
[275] ECtHR July 1, 1961, *Lawless v. Ireland* [1961], 1 EHRR 15.
[276] At the beginning of 1939 the IRA published documents described by it as a 'declaration of war on Great Britain'. Following that declaration, the IRA, operating from territory of the Republic of Ireland, intensified its acts of violence on British territory. In order to meet the situation created by the activities of the IRA, the Parliament of the Republic of Ireland passed the Offences against the State Act, 1939, which came into force on June 14, 1939 (par. 7).

The detainment of Mr. Lawless was not considered:

'*a measure going beyond what was strictly required by the situation at that time.'*

So circumstances are enabling the freedom of legal competence which allows countries to guard their safety in public emergency situations. Although one should be aware that it is not always clear where the line between emergency and semi-normal situation is drawn, certainly the political temperature in the 'democratic society' is not always considered a stable factor. One could expect that the competences of the authorities to intrude on privacy under emergencies are considerably stronger than under otherwise normal situations. But these qualifications are increasingly convergent when terrorist threats are at hand in the 'normal' situation.

Even under semi exceptional circumstances as terrorist threats these measures still have to be proportional and guaranteed by other requirements of due process, fair and scrutinized by a possible independent control mechanism.

A more detailed description from different perspectives is given in the following sections.

4.4.2 Prescribed (and Limited) by Law in the ECHR

One of the most important principles to limit fundamental rights is that those limitations must find their basis in the law. This is specified in Article 8(2) of the ECHR. These limitations are 'specified' in a broad sense. There are various articles within the ECHR, such as the freedoms of thought, expression, association, and the first protocol on possession, which provide specific exceptions .[277] The law that forms the basis of the limitations, can be at any national level and the wording of these texts in the law itself can again, create more possibilities to limit the freedom of the citizen's personal life.

Although there may be limitations provided for within the law, it is not possible to discern whether the importance and proportion of the limitation outweigh the competing interest on the other side.

Christoffersen[278] examines the scope of the proportionality principle from the perspective of limitation clauses. He observes that (logically) several provisions are textual and orientated toward the possible interpretation by the interpreter. The reason is that the exceptions are structured in such a manner so as to invite the interpreter to divide the application of the norms. This will be applied in a two-fold test wherein firstly, the scope of protection is delimited and thereafter the scope of prohibition is determined. Although this is a textual explanation of the clause itself, in case law there is no automatic limitation of the right; more often, the limitation is determined.

This limitation test or 'fair balance' test is applied by the ECtHR to privacy and all other non-absolute fundamental rights which entail the limitation clause. The relevant case law and

[277] Concerning the right of possession there is a slight difference in the wording: Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

[278] Christoffersen 1990, p. 74-75.

scholarly writing on limitations to fundamental rights[279] is discussed later in this chapter.[280] They present the limitations by provisions of this kind on all other freedoms.[281]
These limitations may only be justified if they are 'prescribed by law' and, as previously discussed, this refers to several aspects of the quality of the law as well as to the transparency and accessibility. The wording, as used in Article 8(2) concerning privacy, of 'in accordance with the law' seems to be weak in its protective power. Korff says that the ECtHR has,

> *held that, given the fundamental nature of the Convention rights, the first paragraph should be widely interpreted, and the second one narrowly. Rights must therefore be 'stretched', and limitations limited.* [282]

The difference in wording is, according to Van Dijk and Van Hoof, just a reference to a different formulation, probably based on the difference of a monistic or dualist system, i.e. not per se referring to the national law but also to the international law. [283] It may also be a provision of international law which, in virtue of the monistic system applying within a given state, forms part of its national legal order.[284]

It is also possible that a wider opportunity to limit the Article was intended by its phrasing. 'Prescribed by law' seems to be more specific than 'in accordance with the law'. According to Van Dijk and Van Hoof, different formulations of a sufficient legal basis are irrelevant. The French text 'prevue par la loi' is used for 'prescribed by law' as well as for 'in accordance with

---

[279] the freedom to manifest one's religion or beliefs ('shall be subject only to such limitations…', Article 9 § 2), the freedom of expression ('The exercise of these freedoms … may be subject to such formalities, conditions, restrictions or penalties…', Article 10 § 2), 511 the freedom of assembly and association ('No restrictions shall be placed … other than such as are' Article 11 § 2), derogation ('… may take measures derogating … to the extent strictly required…' Article 15), deprivation of possession ('No one shall be deprived …except … ', Protocol no. 1 Article 1 § 1, first sentence), the freedom of movement ('No restrictions shall be placed … other than such as are …' and 'The rights … may also be subject … to restrictions …' , Protocol no. 4 Article 2 § 3 and Article 2 § 4) and the right to appeal in criminal matters ('This right may be subject to exceptions …', Protocol no. 7 Article 2).

[280] Opsahl 1992, p. 459.
For a similar observation in respect of US constitutional law, see Glendon 1992, p. 41; Schauer 1991, p. 874. Also see: ECtHR October 17, 1986, *Rees v. United Kingdom* [1986] 9 EHRR 56.; 510 ECtHR May 25, 1993, *Kokkinakis v. Greece* [1993]*;* ECtHR December 7, 1976, *Handyside v. the United Kingdom* [1976], Series A no. 24; ECtHR June 22, 1981, *Young, James and Webster v. the United Kingdom* [1981] Series A no. 44.

[281] The freedom to manifest one's religion or beliefs ('shall be subject only to such limitations…', Article 9 § 2), the freedom of expression ('The exercise of these freedoms … may be subject to such formalities, conditions, restrictions or penalties…', Article 10 § 2), 511 the freedom of assembly and association ('No restrictions shall be placed … other than such as are' Article 11 § 2), derogation ('… may take measures derogating … to the extent strictly required…' Article 15), deprivation of possession ('No one shall be deprived …except … ', Protocol no. 1 Article 1 § 1, first sentence), the freedom of movement ('No restrictions shall be placed … other than such as are …' and 'The rights … may also be subject … to restrictions …' , Protocol no. 4 Article 2 § 3 and Article 2 § 4) and the right to appeal in criminal matters ('This right may be subject to exceptions …', Protocol no. 7 Article 2).

[282] D. Korff, *The standard approach under articles 8-11 ECHR and Article 2 ECHR***,** London Metropolitan University, internet text July 2012:
<http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf>.

[283] Van Dijk & Van Hoof, note 266, p. 766.

[284] As is the case with The Netherlands; Article 93: Provisions of treaties and of resolutions by international institutions which may be binding on all persons by virtue of their contents shall become binding after they have been published. Article 94: Statutory regulations in force within the Kingdom shall not be applicable if such application is in conflict with provisions of treaties that are binding on all persons or of resolutions by international institutions.

the law'.[285] Still there is a difference in wording; e.g. the possibility to have a police investigation for general purposes as defined in the Article 3 of the Dutch Police Act:[286] '*The police have the task to maintain legal (…) order*.[287] So general descriptions are in accordance with the law and not (specifically) described by the law.

The concept of 'in accordance with the law', also refers to general descriptions in national law, as well as to the more open-ended articles of international conventions, as in this case which applies to Article 8. According to the introduction of a special Article 8 ECHR blog in the UK:

> *Article 8 is one of the most open-ended of the Convention rights, covering a growing number of issues and extending to protect a range of interests that do not fit into other Convention categories. This is partly because neither the Commission, when it was still in existence, nor the Court in its present incarnation, have attempted any comprehensive definition of Article 8 interests, adapting them to meet changing times.*[288]

This blog-post is an example of the perception of Article 8. The (negative) obligation not to interfere with privacy rights still offers the opportunity to restrict the right of privacy and personal life on the basis of the law as a general concept constrained by discretionary powers.[289] It could even mean 'within the spirit of the law', not taking it literarily… If the boundaries of 'non-intervention by the State' are more or less blurred it is hard to decide that a State is intruding the fundamental right on privacy. What is at stake, according to Van Dijk and Van Hoof –is that the ECtHR is "ensuring respect for the rule of law, and providing protection against the opposite of the rule of law: arbitrary power (or unfettered discretion). These very basic considerations inform the thinking of the Court throughout its standard assessments."[290]

In terms of registering persons, Van Dijk and Van Hoof hold that the activity "

> *does not conflict with Article 8, not even when the registration concerns persons who do not have any criminal record*."[291]

Although this is referring to a case from 1973, the interpretation seems to be even more applicable in the information age, e.g. concerning the mentioned storing of car license plate registrations by the police on the public road in order to detect criminal activities by comparing data files of Automatic Number Plate Recognition (ANPR) for any future police purposes. In The Netherlands, since 2009, cameras have registered much data on behalf of the ministry of

---

[285] Van Dijk & Van Hoof, referring to judgement of March 25, 1983, Silver and others, A.61, pp. 32-33; judgement of 2 August 1984, Malone, A82, p.31, as well as in: the Commission Report of 11 October concerning, Silver, B.51 (1987), p. 74; in note 269 and 270.

[286] Article 3 of the Dutch Police Act, *see also* Van den Hoven van Genderen 2008, p. 28.

[287] Article 3 Dutch police act:, replacing Article 2 (2011): The police has the task in submission to the authorities and in accordance with the law, to care for the actual maintenance of the legal order and the ministering of help to those who are in need of help.

[288] A. Wagner a.o., *Article 8, Right to private and family life,* <http://ukhumanrightsblog.com/incorporated-rights/articles-index/Article-8-of-the-echr/>.

[289] Consisting of the elements of privacy as discerned: ((1) private life; (2) home; (3) family; (4) correspondence.

[290] Korff, p. 1.

[291] Van Dijk & van Hoof, p. 491 note, ref. Appl. 5877/72 *X v. the United Kingdom*, Yearbook XVI (1973), p. 328 (388), where the complaint concerned the taking, and storing in a file, of photographs of the applicant by the police for possible future identification purposes. The Commissions evidently considered it decisive here that the photographs had not been released for publication or used for purposes other than police ends.

transport in order to detect traffic jams and has been used by the ministry of finance for tax reasons. The police and information agencies have used this information, connected to other personal data, for activities supporting the general task of the police and the security agency, and particularly to detect criminal acts.[292].

The fact that ANPR can be used for crime prevention in a broad sense, opens doors for fishing expeditions and function creep that can be considered a breach of privacy, particularly when relying on the sophistication of cameras to discern innocent people from suspected criminals.

4.4.3 Detournement de Pouvoir or Legitimized Limitation?

Van Dijk and Van Hoof question the grounds of restrictions and put forward that a review of the collection and use of data would be a *detournement de pouvoir*. This was the situation in the case X v. Austria in which the Commission considered the transmission of personal data by the police to the criminal court justified in the interest of the prevention of crime, although the case concerned the prosecution of crime and not its prevention.[293] The first paragraph of Article 8 was not under consideration because the Commission did not doubt the applicability of par. 2 of Article 8 ECHR and therefore did not consider positive action by the state to protect the right of the first paragraph.

> *The Convention gives protection against certain interventions by the State (Staatliche Eingriffe) but it does not guarantee a right of an individual to ask the State to take certain action in his interest.*

Doubts of the just application of the second paragraph also seem to vanish if the motivation lies within the perimeter of prevention of terrorism. We see in those cases where national security causes infringement of Article 8 that (secret) surveillance and other interferences with personal life and communication can be justified as long as they are 'strictly necessary for safe-guarding the democratic institutions.'[294]

This wording means that permission and therefore limitation by law has to be clear and objective. In the case of Valenzuela Contreras v. Spain of 1998, concerning wire-tapping, there were doubts about the wording and application of the legal norms:

> *'the legislature [had] not specified any limitations according to the nature of the possible offence or the sentence it carried' and emphasised that the deficiencies, inadequacies*

[292] CBP guidelines, *The Application of automatic recognition of license plates by the police* 2009 (The national Personal Data Protection Authority (CBP) has criticized and denied an earlier draft Act on the reasons of misuse of police competence. The CBP therefore developed guidelines how to use ANPR . Initially, the Act is directed against traffic crimes and fugitive criminals as is described in the 'privacy assessment report' (PAR), but if necessary could be used for other police tasks. The period of storage (four weeks) and the purpose can be easily changed for other police purposes. I have serious doubts about these kind of activities. It is questionable if restricting privacy by using and matching of different data files is allowed under Article 8, even within the concept of 'accordance with the law'

[293] Van Dijk & van Hoof 1979, p. 491.

[294] Greer 1997, p. 19 (In 1978 the Court observed in Klass that two then comparatively recent developments, including technical advances in espionage and the development of European terrorism, had made secret surveillance particularly necessary).

and vagueness of that legislation needed to be rectified by the case-law of the domestic courts and of the European Court of Human Rights. [295]

The (Spanish) Supreme Court had concluded that mere suspicion was not enough evidence for restricting a fundamental right as privacy by tapping the telephone and there was no sufficient judicial supervision.[296]

Since the attacks of September 11, 2001, there has been a general acceptance of the invocation of 'suspicion' as a justification for the use of intrusive techniques. As is accepted in nowadays (after 9/11) criminal (investigative) law, is not deemed sufficient since this decision.

In later case law[297] the ECtHR decided that, concerning the application of the general principles concerning case-law interferences of Article 8(2), restrictions have to be in accordance with the law, referring not merely to the existence and the accessibility of the law by the persons concerned, but also to the quality of the law.[298]

This case is particularly interesting for its reference to the special position of an (executive) party using means to secretly survey or investigate the personal sphere (including any communications) of citizens. In those cases, a fair risk of 'detournement de pouvoir' is accounted for and guarantees against this have to be made clear.[299]

---

[295] ECtHR 30 July 1998, *Valenzuela Contreras v. Spain* [1998] 28 EHRR 483.

[296] *In summary, the violations that render evidence obtained from telephone tapping inadmissible and determine its effects are as follows:*

(1) Lack of evidence. Lack of sufficient reasoning

Lack... of evidence capable, in the judge's view, of justifying a measure restricting fundamental rights to the extent telephone tapping does; mere suspicion on the part of the police, which in principle serves as the basis for the court's decision, cannot suffice.

(2) Lack of supervision

There was an almost total lack of any form of judicial supervision of the actual monitoring of the telephone concerned, which must necessarily be effected in compliance with the proportionality principle (...) and a decision taken as to whether or not expressly to extend the measure/surveillance – which, moreover, should not be for more than a reasonable period – in accordance with the principles laid down by the Code of Criminal Procedure.

[297] Par. 46. *(i) The interception of telephone conversations constitutes an interference by a public authority in the right to respect for private life and correspondence. Such an interference will be in breach of Article 8 § 2 unless it is 'in accordance with the law', pursues one or more legitimate aims under paragraph 2 and, in addition, is 'necessary in a democratic society' to achieve those aims (see the Kopp v. Switzerland judgement of 25 March 1998, Reports 1998- II, p. 539, § 50).* And: The investigating judge had consequently anticipated the safeguards and guarantees against arbitrariness specified in the Kruslin v. France and Huvig v. France judgements five years before those judgements were delivered.

[298] (ii) The words 'in accordance with the law' require firstly that the impugned measure should have some basis in domestic law. However, that expression does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law. The expression thus implies that there must be a measure of protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 (see the Malone judgement cited above, p. 32, § 67). From that requirement stems the need for the law to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see the Kruslin judgement cited above p. 20, § 27, and the Kopp judgement cited above, p. 540, § 55).

[299] (iii) Especially where a power of the executive is exercised in secret the risks of arbitrariness are evident. In the context of secret measures of surveillance or interception by public authorities, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such

Referring, several minimum safeguards should be set out in the statute in order to avoid abuses of power are mentioned consequently by the Court. These safeguards can increase the control as well as legal certainty for the subjects:

- a definition of the categories of people liable to have their telephones tapped by judicial order,
- purpose definition of the measures taken
- the nature of the offences which may give rise to such an order,
- a limit on the duration of telephone tapping, possible storage duration and purposes
- the procedure for drawing up the summary reports containing intercepted conversations,
- the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence and
- the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court.[300]

Although in this case the investigating judge attempted to ensure maximum protection with respect to the enforcement of the monitoring order under the legal provisions in force at the time, the Court notes that some of the conditions necessary under the Convention to ensure the foreseeability of the effects of the 'law' and, consequently, to guarantee respect for private life and correspondence, are not included.[301]

Even though the new regulations gave more guarantees, the sensitivity of the intrusion and insufficient provisions according to the requirement of the Convention resulted in a negative verdict for the State of Spain.

Would this reasoning be different in cases of state security?

In order to give an example of the difference in argumentation in applying limitations on the basis of Article 8(2) for reasons of state security or for reasons of crime prevention legislation, I refer to the case of Telegraaf v. The Netherlands of 2013. State secrets obtained from investigations of The Netherlands secret service, AIVD[302], came to circulate in the criminal circuit of Amsterdam.[303] Journalists at the Dutch newspaper, De Telegraaf, published this

[300] See: loc. cit. p. 24, § 35, and p. 56, § 34, respectively.
[301] Ibid [56].
[302] General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst).
[303] The Minister wrote to the Lower House on 20 December 2006. His letter concluded as follows:
'*There has been what can properly be called a serious incident*' (Er is sprake van een ernstig incident geweest): a considerable collection of copied documents from a closed working file of the BVD has been taken out of the building in defiance of the rules. Operational AIVD research and research by the National Police Internal Investigations Department (Rijksrecherche) indicate that this was probably done by a former BVD staff member, who would have had the opportunity to do so until August 2000. Possibly via third parties, the documents subsequently came into the possession of De Telegraaf, which published information about this in January of 2012. I would point out that final conclusions about the way in which these compromising facts took place can formally be drawn only when the proceedings against the suspected former staff member have been brought to a close. The compromised documents provide an insight into the BVD's operational knowledge levels at that time within the task area of public-sector integrity and in the BVD's working methods relating to that task area. Damage to investigations in process and the consequences of the working methods then in use (modus operandi) becoming known is relatively limited. Risks to agents and/or informants cannot however be excluded. Where necessary, operational measures have been taken to limit these risks.

information, endangering the position of infiltrated policemen. It appears from the documents that the AIVD considered top criminal Mink K. to be a threat to the legal order as he reserved millions each year to bribe police and prosecution service officials. In addition, K. was thought to have enormous stocks of weapons at his disposal, including large quantities of semtex and 'hundreds of anti-tank missiles'. The links which K. was thought to maintain with terror groups such as Hezbollah and ETA were, moreover, worrisome. The documents were returned to the AIVD by De Telegraaf.[304]

The Supreme Court accepted the ruling of the Court of Appeal, that in the case of state security, to the scales tend to balance in favour of the *'overriding requirement in the public interest'*.

The Supreme Court stated:

> *'3.7.3. (...) The Court of Appeal has not overlooked the fact that the interests of the Government invoking one of the exceptions set out in Article 8 § 2* [ECHR]*and Article 10 § 2, if they are to justify such an exception, must tip the balance against the interests in maintaining the rights and freedoms guaranteed by those provisions. (...) such use is only justified by an undeniable need in the public interest unambiguously implies that the Court of Appeal, in applying its test, has had regard to the condition, formulated by the European Court of Human Rights, of an 'overriding requirement in the public interest'.*

Most interesting is the report by the Supervisory Board that was presented to the Minister on 15 November 2006. This report was classified state secret which is the second-highest classification level for state secrets. The Government quotes that the Intelligence Service (AIVD) may come across information that is important for criminal investigations. Even if the service has received this information by the use of their extended powers they still have the right to hand it to the public prosecution.*[305]*

The different competences of the ministry of justice, *in casu* the police and public prosecution office, and the secret service, in *casu* the AIVD, seem to have no barriers between each other. That is, there are no impediments in exchanging information amongst the bodies. The fact that the secret service has no investigative powers for the purposes of criminal investigation is simply set aside. Likewise, there are instances wherein the police make use of information gathered by the Secret Service, thereby circumventing the legally-required court order that should have been obtained if they would have initiated the tapping themselves.

Concerning this 'adulteration' with the investigation headed by the Public Prosecution Service, the earlier mentioned supervisory board (commissie van toezicht) is of the opinion that the use of special powers in the present case fell within the task of the AIVD as set out in section 2.2(a) of the 2002 Intelligence and Security Services Act. The special powers have thus not been used

---

[304] ECtHR 22 February 2013, *Telegraaf Media Nederland Landelijke Media B.V. and others v. The Netherlands* [2013], Application no. 39315/06.

[305] *'[Section 9(1) of the 2002 Intelligence and Security Services Act] provides that public servants of the AIVD do not have the power to conduct a criminal investigation. The AIVD is therefore not entitled to employ any special powers with the aim of a criminal investigation. (...)Although the AIVD investigation is not aimed at collecting evidence for criminal proceedings, in performing its task the AIVD may come across information that may also be important for the criminal investigation and prosecution of criminal offences. In that case the AIVD based on [section 38 of the 2002 Intelligence and Security Services Act] has the possibility to make available the information to the [Public Prosecution Service] via an official message to the National Public Prosecutor for Counter-terrorism. In the investigation in hand several official messages were issued to the [Public Prosecution Service].*Ibid [39].

for the purpose of the criminal investigation. The issuing of official reports (ambtsberichten) in this case cannot lead to the finding that there has been amalgamation or adulteration of tasks and powers between the AIVD and the Public Prosecution Service. After all, this concerns the regular provision of information – which the AIVD had obtained based on its own tasks – to the Public Prosecution Service in accordance with the law in force.

Although it is interesting in the sense of the freedom to gather information and the special position of journalists concerning protecting their information to this freedom of the press, not disclosing their source, it is not my intention to elaborate on this aspect.[306] The ECtHR ruled that although the investigative powers of the AIVD, are considered legitimate, this does not extend to infringing on the rights of journalists and specifically the protection of their sources.[307] For this thesis it is more important to explain the limitation of the right to privacy and therefore the validity of the application of Article 8(2) in the ruling of the ECtHR, although the Court finds Articles 8 and 10 closely intermingled and difficult to separate in this case.[308]

4.4.4 Quality of Law Also Means no Arbitrary Interference by Public Authorities

The ECtHR in the aforementioned case, with regards to limiting both Articles 8 and 10 'in accordance with the law', reiterates that measures taken must have some basis in domestic law and be understandable and accessible to the people subject to it.

Also in this case the importance of transparency of the rules of competence of the executive authority is stressed, certainly when it considers 'secret activities'. There always has to be a democratic guarantee against arbitrariness and function creep.[309]The Court made clear that

[306] Ibid [60]: Several international instruments concern the protection of journalistic sources; among others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and the Resolution on the Confidentiality of Journalists' Sources by the European Parliament (18 January 1994, Official Journal of the European Communities No. C 44/34).61.

[307] Ibid [86]. The Court is prepared to accept that the AIVD's purpose in seeking to identify the person or persons who had supplied the secret documents to the applicants was subordinate to its main aim, which was to discover and then close the leak of secret information from within its own ranks. However, that is not decisive (see ECtHR 14 September 2010, *Sanoma Uitgevers B.V. v. The Netherlands* [2010], no. 38224/03, § 66,). The Court's understanding of the concept of journalistic 'source' is 'any person who provides information to a journalist'; it understands 'information identifying a source' to include, as far as they are likely to lead to the identification of a source, both 'the factual circumstances of acquiring information from a source by a journalist' and 'the unpublished content of the information provided by a source to a journalist' (see Recommendation No. R(2000) 7 on the right of journalists not to disclose their sources of information (quoted in paragraph 61 above); compare also Sanoma, §§ 65-66, and Weber and Saravia, §§ 144-45).
As in Roemen and Schmit v. Luxembourg, no. 51772/99, § 52, ECHR 2003-IV; Ernst and Others v. Belgium, no. 33400/96, § 100, 15 July 2003; Tillack v. Belgium, no. 20477/05, § 64, 27 November 2007; and Sanoma, loc. cit., the Court must therefore find that the AIVD sought, by the use of its special powers, to circumvent the protection of a journalistic source (compare and contrast Weber and Saravia, § 151).

[308] *Telegraaf* par. 88.

[309] *The law must be compatible with the rule of law, which means that it must provide a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded by Article 8 § 1 and Article 10 § 1. Especially where, as here, a power of the executive is exercised in secret, the risks of arbitrariness are evident. Since the implementation in practice of measures of secret surveillance is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual*

investigations by the secret services have a risk to potentially harm the democratic values of the society and therefore require the clear supervision of an impartial supervisory body.[310]If not, there is a severe risk to harm democracy based on the freedom of information and the protection of personal privacy.

The Court further determined that there had been an 'interference' with the first applicant's freedom to receive and impart information, and that this finds a basis in Dutch law, under Article 96a of the Code of Criminal Procedure.[311] Nevertheless, the aims pursued by the interference were, at the very least, 'national security' and 'the prevention of crime' according to the government.

The test of 'necessity in a democratic society' requires, according to the Court, a degree of appreciation which complements the approach of the ECtHR

> 'whose task it is to give a final ruling on whether a restriction is reconcilable with freedom of expression as protected by Article 10."[312]

The ordering of the return and seizure of the documents and the alleged investigative actions are not considered 'relevant and sufficient' reasons for the interference done by the State. It would have been significant if the Court had investigated…", the most serious aspect of the so called 'adulteration of investigative powers' between the prosecutor's office and the secret service, although it can be perceived that the Court already stated that the guarantees of an independent supervisory authority and a legal ground of transference of the information should be enough ground for evaluating and adapt this part of the criminal (procedural) law.
There have been proposals to support the police with comparable authority and competences that the secret service already have, probably because the secret service already has the ability to inform police on the basis of the information acquired by the AIVD.[313]

---

adequate protection against arbitrary interference See alsoWeber and Saravia, §§ 93-95 and 145; Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, § 76, ECHR 2006-VII; Liberty and Others v. the United Kingdom, no. 58243/00, §§ 62-63; 1 July 2008; Kennedy v. the United Kingdom, no. 26839/05, § 152, 18 May 2010, par. 90.

[310] Ibid [98]. The Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8, that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see Klass and Others v. Germany, 6 September 1978, § 56, Series A no. 28, and Kennedy, cited above, § 167). However, in both cases the Court was prepared to accept as adequate the independent supervision available. In Klass and Others, this included a practice of seeking prior consent to surveillance measures of the G 10 Commission, an independent body chaired by a president who was qualified to hold judicial office and which moreover had the power to order the immediate termination of the measures in question (mutatis mutandis, Klass and Others, §§ 21 and 51; see also Weber and Saravia, §§ 25 and 117). In Kennedy (loc. cit.) the Court was impressed by the interplay between the Investigatory Powers Tribunal ('IPT'), an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, and the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office (Kennedy, § 57) and who had access to all interception warrants and applications for interception warrants (Kennedy, § 56), para.100.

[311] Concerning the journalists prerogative or legal privilege not to divulge their source of information;Para. 119, referring to ECtHR 14 September 2010, *Sanoma Uitgevers B.V. v. The Netherlands* [2010], no. 38224/03, § 66.

[312] Ibid [215].

[313] Note 188: Parliamentary white papers, 30164, nr. 3, 2004-2005, Change of the Dutch Code Criminal Code, Code of Criminal Procedures and other laws to extend the possibilities to discover and prosecute terroristic crimes, p. 5/6 (Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven). Also in the so called 'Computer crime III'proposals of 2015, extension of search competence in the sense of placing spy software is foreseen.

4.4.5 Limitations of Article 8: Necessary in a Democratic Society

Limitations and intrusions upon the personal right to privacy have to be within certain limits as described above. In all cases, the activities by authorities and other arms of government have to fall within the scope of being 'necessary in a democratic society.' The references to necessity in a democratic society were already introduced in the alternative draft presented by the British Government of the text of the ECHR.[314] These qualifications apply equally to Articles 9, 10 and 11. The limitations to those fundamental rights, as in the protection of personal data as guaranteed by Article 8 of the Convention, must afford appropriate domestic safeguards to prevent any such use of personal data to begin with.

The principles of proportionality and purpose are strongly tied to the principles of 'in accordance with the law'. However, most case law reasoning falls back on the umbrella theme of the democratic society. 'Accordance with the law' or 'prescribed by law' relate to five points which are supported by the case-law of the ECtHR:

(1) There must be a specific legal rule or regime which authorises the interference with a legitimate aim. For intrusive actions such as the interception of telecommunication I refer to the Aalmoes case. Domestic law has to provide for various procedural safeguards designed to ensure that the interception of telecommunications is not ordered haphazardly, irregularly or without due and proper consideration. It requires this measure to remain under the permanent supervision of a judge as also made clear in the cases of the Telegraaf group and Valenzuela Contreras v. Spain;
(2) The citizen must have adequate access to the law in question (The Sunday Times v United Kingdom); that means it must be comprehensible and accessible.
(3) The law must be formulated with sufficient precision to enable the citizen to foresee the circumstances in which the law would or might be applied as well as its consequences (Sunday Times and Malone v United Kingdom).
(4) The law must be necessary in a democratic society. As such the limitation must support the legitimate aim as a pressing social need of the society.
(5) Finally, the law must not unduly intrude upon the democratic value of the society, meaning that the limitation and consequent intrusion are proportional and that there are no other (lesser intrusive) means to reach its purpose (subsidiarity/minimalisation).

If these thresholds are met there is still one overarching consideration of the court: are the measures, though legitimate, in favour of the individual?

4.4.6 Balancing the Rights by the Principles

In analysing the case law of the ECtHR, the most important process concerning the limitation of rights is the (fair) balancing test which hinges on the basis of proportionality. Proportionality entails comparing the use of means with the relative importance of the rights of concerned parties. According to Christoffersen, the use of this balancing test by the ECtHR was based on the development of a new mood towards the end of the 1970's.[315] The point is that proportionality is always based on the weighed importance of different norms and interests, so one is never sure what is deemed the most important, from a neutral position, when conflicting

[314] Christoffersen 1961, p. 516-19; Simpson 2001, p. 715.
[315] Christoffersen 2009, p. 68.

norms and interests are put on the scale by national authorities in the application of the limitations, and even when this balancing process is executed by the ECtHR.

The margin of appreciation of the concept 'necessity in a democratic society' is influenced by the state of mind of the authorities and the appreciation of the circumstances at hand. With reference to Christoffersen, democratic society can be understood as the protection of societal interests. This is described in different terms that are generally very flexible such as 'the general interest,' 'common good' and 'the public interest'; equally vague is the notion of 'democratic society.' [316]

Even if a measure has been selected in pursuit of one of the legitimate interests listed in the second paragraph of Articles 8, 9, 10 or 11, the measure must be tested for 'necessity'. The Court has held that the notion of necessity implies two things:

(1) that an interference corresponds to a pressing social need;
(2) That it is proportionate to the legitimate aim pursued, and meaning that the reasons provided by the national authorities to justify it are 'relevant and sufficient'.

These provisions of 'necessity' have been more strongly worded by the likes of Korff who stated that interference may 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.[317]

In first instance it is for the national authorities and the independent courts to decide if the reasons adduced by the national authorities to justify it are 'relevant and sufficient' by making an initial assessment in all these respects. The final evaluation of whether the interference is necessary remains subject to review by the Court in terms of its conformity with the requirements of the Convention.[318]

4.4.7 Margin of Appreciation, Proportionality Test

Of course at the first instance an assessment of the margin of appreciation must be left to the competent national authorities. The question remains how far this competence is allowed to reach. The breadth of this margin varies and depends on a number of factors including the nature of the fundamental right, its importance for the individual, the nature of the interference and the objective pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights as was made clear by the decision in the Connors case.[319]This case considered the eviction of a gypsy family, breaking article 8(1) without taking into account the specific requirements for the minority group. Also the apply for judicial review was refused to Connors by the authorities.. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the state will be restricted.[320] When, however, there is no consensus within

[316] Reference to *Human Rights and the End of Empire - Britain and the Genesis of the European Convention* 2001, pp. 662 ff. and Protocol no. 1 Article 1 (property); Protocol no. 1 Article 1 (property), Protocol no. 4 Article 2 (movement), and Protocol no. 7 Article 1 (expulsion procedure).
[317] See Korff 2008.
[318] See ECtHR 18 January 2001, *Coster v. the United Kingdom* [2001], App no. 24876/94, § 104.
[319] See ECtHR 27 August 2004, *Connors v. the United Kingdom* [2004], App no. 66746/01, § 82.
[320] § **Fout! Alleen hoofddocument.**. The serious interference with the applicant's rights under Article 8 requires, in the Court's opinion, particularly weighty reasons of public interest by way of justification and the margin of appreciation to be afforded to the national authorities must be regarded as correspondingly narrowed. And:
ECtHR 10 April 2007, *Evans v. the United Kingdom* [2007], App no. 6339/05, § 77.

the member states of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin of appreciation will be wider.[321] The Connors case notes that, for example, in terms of the application of social or economic policies, the margin of appreciation can be quite wide, although in this specific case not too wide.[322]

4.4.8 Proportionality in Investigations of Personal Information in Stored Files

This aforementioned margin of appreciation is often, for a significant part, based on the principle of proportionality.[323] When concerning the protection of personal data undergoing automatic processing, the need for safeguards is great. It is all the more significant when such data are used for police purposes.[324] The domestic law should ensure that such data are relevant and not excessive in relation to the purposes for which they are stored and ensure that the data are 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.[325]

The domestic law must also afford adequate guarantees that retained personal data is efficiently protected from misuse and abuse as referred to in several instruments of ECHR legislation.[326] The considerations outlined above are especially valid with regard to the protection of special categories of more sensitive data[327] and particularly of DNA information.[328] The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprints and DNA information, may be outweighed by the legitimate interest in the prevention of crime.[329] However, the intrinsically personal and private character of this information calls for the Court to exercise careful scrutiny of any state measure authorising its retention and use by the authorities without the consent of the person concerned.

The compiling, storing, using and disclosing of personal information by the state, for example with respect to a police register, amounts to an interference with one's right to respect for private life as guaranteed by Article 8 (1) of the Convention.[330] The subsequent use of the stored information has no bearing on that finding, as confirmed in the *Amman* case.[331] Such interference breaches Article 8 unless authorities pursue one or more of the legitimate aims referred to in paragraph 2, according to the requirements as stated in section 4.4.4 to achieve those aims. In the case of *Uzun*,[332] the Court came to the conclusion that the applicant's surveillance in all thinkable ways, including the interception of all communication, transmitters placed in his car (pfeilsenders), secret camera's and surveillance via GPS, was disproportionate to the purpose. Nevertheless this action was permitted by the Federal Public Prosecutor General in order to investigate several counts of attempted murder for which a terrorist movement had

[321] See ECtHR 4 December 2007, *Dickson v. the United Kingdom* [GC], App no. 44362/04, § 78.
[322] See ECtHR 27 August 2004, *Connors v. the United Kingdom* [GC], App no. 66746/01. § 86
[323] Christoffersen 2009, p. 70.
[324] See Korff 2008.
[325] See later in this paragraph, Article 5 of the Data Protection Convention and the preamble thereto and Principle 7 of Recommendation R(87)15 of the Committee of Ministers regulating the use of personal data in the police sector.
[326] See notably Article 7 of the Data Protection Convention.
[327] See Article 6 of the Data Protection Convention.
[328] See Recommendation No. R(92)1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system.
[329] See Article 9 of the Data Protection Convention.
[330] Confirmed in:ECtHR 26 March 1987, *Leander v Sweden* [1987] 9 EHRR 433, para 48.
[331] ECtHR 16 February 2000, *Amann v. Switzerland* [2000], App no. 27798/95, para 69.
[332] ECtHR 2 December 2010, *Uzun v. Germany*, App no. 35623/05.

claimed responsibility and to prevent further bomb attacks. This served the interests of national security and public safety, the prevention of crime and the protection of the rights of the victims. In the end the interference was proportionate to the legitimate aims pursued and thus '*necessary in a democratic society*' within the meaning of Article 8(2).

The Düsseldorf Court of Appeal raised an interesting point in terms of the balancing act that is required in determining proportionality. This Court determined that, according to the Code of Criminal Procedure, surveillance via GPS did not have to be ordered by a judge, as opposed to measures interfering more profoundly with the right to self-determination in the sphere of information. Whether or not a surveillance measure could be ordered in addition measures already in place was a question of proportionality of the additional measure in question.[333]

That is to say, the use of extra surveillance measures was not considered to be a deeper intrusion on the privacy of the individual because the intrusion already was in place. If this still would be proportional to the purpose that is served by the measure, then it is considered tolerable. More generally, the acceptance of the spectrum of instruments that will be used is, in first instance the prerogative of the authorities. Where personal information is stored in the interests of national security, there should be adequate and effective guarantees against abuse by the state. Where such safeguards do exist, the Court will not necessarily find a violation of Article 8. Telecommunications data is widely used by state authorities for surveillance purposes since it can be stored and accessed at hardly any cost.[334] Public authorities now have the possibility to use this filed information on basis of the Retention regulations, although they are contested by several European States and the European Court of Justice ruled the retention directive invalid as will be explained later.[335]

Evidently a more clear consideration of this sort is to be found in the Leander case where the 'secret police' register contained information about the private life of Mr. Leander. The opinion of the Court was that the protection of national security was of such importance that interference in the private life (at least this was not contested) demanded this intrusion. Subsequently the Court concluded:

> Having regard to the wide margin of appreciation available to it, the respondent State was entitled to consider that in the present case the interests of national security prevailed over the individual interests of the applicant. The interference to which Mr. Leander was subjected cannot therefore be said to have been disproportionate to the legitimate aim pursued.[336]

The Gaskin case it concerned the refusal of admission to the personal files of Mr. Gaskin on basis of the fact that (confidential) public files under circumstances should not be accessed if other interests (of the state or third parties) could be endangered. The Court decided that, taking into account the state's margin of appreciation of the obligations under Article 8, a fair balance between the general interests of the state and the rights of individuals should be protected by the state, as this is secured in the Convention and any intrusion must be in conformity with the principle of proportionality. Part of this 'system' to determine proportionality should also be that there is an independent overseeing authority to decide if this is the case. In the Gaskin case

[333] Ibid [para. 14].
[334] See: Council of Europe/European Court of Human Rights, 2011 (7) Internet: Case-law of the European Court of Human Rights.
[335] See also chapter 5.3.1 concerning the retention directive.
[336] Van Dijk & Van Hoof, note on p. 492, concerning *Leander v. Sweden,* par. 22.

there was no such procedure available. As we have seen in many cases, the availability of independent control mechanisms is considered essential in the limitation of privacy.[337]

It is interesting to see that the Court connected the principle of proportionality, to the principle of having an impartial independent authority that must oversee or even must decide this balance of taking the just measures under the circumstances.

4.4.9 Professional Secrecy? (Trust Exception)

The 'lex specialis' in this section concerns the privileged relationship between lawyers and their clients in terms of private communications. It is understandable that prosecutors and investigators look for 'workarounds' to obtain information about the possible suspects of criminal activities and those who defend them. On the other hand, the essence of a privacy-orientated democratic society entails that everyone has the right to defend himself by trusted legal professionals against intrusions by the state, certainly in the case of the defense against the suspicion of committed crimes. As such, intercepting the private communications between a lawyer and her/his clients constitutes an intrusion. The Aalmoes and Niemetz cases before the ECtHR, are particularly relevant here. One may expect that the private conversations and information with his lawyer are secret. Intercepting these private communications therefore is creating an intrusion to this very private relation between a lawyer and his clients.

The Aalmoes case, elaborates upon the privacy principles that specify this sensitive privacy relation as in the Niemitz case.

More important, having regard to the materials that were in fact inspected, the search impinged on professional secrecy to an extent that appears disproportionate in the circumstances;[338]

The intrusion of the authorities into the lawyer-client relationship in the Niemitz case had negative repercussions to the legal system as a whole (and the rights of Article 6 of the Convention (right to a fair trial) as well). In the judgment of 29 June 1993, The Netherlands Supreme Court held that lawyers have a professional obligation to secrecy, and thus enjoy the privilege of non-disclosure under Article 218 Dutch Criminal Code of Proceedings (CCP), unless they (the lawyers) themselves are suspects.[339] This was confirmed in a judgment given on 12 January 1999, where the Supreme Court ruled that, pursuant to Article 125h(2) of the CCP, information obtained by tapping telecommunications that falls within the ambit of the privilege of non-disclosure under Article 218 of the CCP. This information cannot be used in criminal proceedings and that, in the case at issue, the trial court had unjustly used in evidence the contents of telephone conversations between a co-accused and his lawyer. The Supreme Court considered that Article 125h (2) was aimed at protecting the interests of everyone in having the possibility to consult a lawyer in all liberty, and without fear of something becoming public which had been entrusted to a lawyer in the latter's professional capacity. According to

[337] *Such system can only be in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case. Accordingly, the procedure followed failed to secure respect for Mr. Gaskin's private and family life as required by Article 8 of the Convention. There has therefore been a breach of that provision* Judgement of 7 July 1989, p.20, note Van Dijk & Van Hoof, p. 493.

339 Nederlandse Jurisprudentie (Netherlands Law Reports – 'NJ') 1993, no. 692.

the Supreme Court, this principle would be impaired if a third person had to take account of the possibility that information entrusted to a lawyer might become known to others, even if this would occur in a procedure to which he or she was not a party.[340]

The effects and seriousness of the intrusion was also clearly influencing the decision in the Kruslin and Huvig case where the measure of intrusion was not only weighed against the proportionality of the measure but also against the specifics of the law; it must be very clear and transparent how the applicable law or regulation is specified and used by the authority. In this case [Kruslin] it concerned telephone conversations that were tapped/intercepted and that act is considered a 'serious interference with private life and correspondence and must accordingly be based on a 'law' that is particular precise. "Further it is interesting to see that the court stated that it is essential to look at the intrusion aspect of the used technology where it seems to be required to have more specific procedures if the technology evolves towards more intrusive techniques as cited in paragraph 4.3 of this book.[341]

In this case, the use of the interception instruments constituted a clear infringement of Article 8 because no specifics on the use of certain technology were laid down in the legislation.[342] This remark is contrary to the reasoning in the *Uzun* case as mentioned above. The extension of use of technologies was tolerated as being proportional. In the *Aalmoes* case the measurement of the technologies used was considered to be an aspect of the quality of the law.

The fact that technology is giving easier access to private life with the increasing possibilities by digital technology would, in the view of the court, require very specific regulation with ample guarantees for a just balancing process.[343]In Dutch criminal law no such balancing took place. In the *Aalmoes case* the ECtHR ruled that the system and law according to interception was partly sufficient, i.e. within the context of a democratic society as far as it considered the interception process as such, but not relating to the aspect of the obligation of destruction of data within the legal rules and obligations. Although the Court ruled the Applicants challenge inadmissible, the case contains some very interesting observations.

The Rotterdam Regional Court took oral evidence on 12 and 17 October 2000 from police officer A.B. on the criminal investigation that was conducted, in the course of which telecommunications with a lawyer - falling within the ambit of the privilege of non-disclosure by virtue of Article 218 of the Code of Criminal Procedure - apparently had been intercepted and recorded. Within the Dutch Justice (prosecutor) policy practice it had then been agreed to record such conversations but not to transcribe them. Further, those recordings of conversation have to be destroyed and may not be brought to court. The officer further declared that it was

[340] ECtHR 24 November 2004, *Aalmoes & others v.The Netherlands* [2004], App no 16269/02. Published in NJ 1999, no. 290, see also p.18.
[341] Van Dijk & Van Hoof, p. 539. Judgement of 24 April 1990, A.1776-A, p. 23 and A176-B, p. 55 respectively.
[342] Having regard to the judgement of the European Court of Human Rights in the Kruslin case delivered on 24 April 1990 and transmitted the same day to the Committee of Ministers; Recalling that the case originated in an application against France lodged with the European Commission of Human Rights on 16 October 1985 under Article 25 of the Convention by Mr Jean Kruslin, a French national, who complained of telephone tapping carried out during a criminal procedure instituted against him; Recalling that the case was brought before the Court by the Commission on 16 March 1989; Whereas in its judgement of 24 April 1990 the Court unanimously:- held that there had been a violation of Article 8 of the Convention.
[343] *Aalmoes* p. 25: In order to secure respect for this reasonable expectation(of protection and respect for their professional privacy), it is therefore required that the interception of telecommunications be subject to an adequate system of supervision. In this area, faced with evolving and sophisticated technology and the possibility of human error or abuse, the Court considers that it is in principle desirable to entrust the supervisory control to a judge.

technically not possible to prevent such conversations from being intercepted. The Rotterdam Regional Court ruled as follows:[344]

> It has been established that there has been a lack of clarity between the public prosecution service and the petitioners about the manner in which an order for destruction must be carried out. It has also been established that deleting [digital data] can be effected in various manners and that not all manners are effective, as has appeared in the [criminal proceedings before the Almelo Regional Court]. The instruction does not prescribe in what manner the destruction must take place. In the explanation to the Instruction a reference is made to the explanation attached to the Decision [on the storage and destruction of items not added to the case file], where it is stated that simply deleting [digital] files is not sufficient, but that the data carrier must be processed in such a manner that the destroyed data can no longer be recuperated.

On the basis of this case, and with the intention to create a clear situation for the sensitive communication between professionals in the law office and their clients, the Dutch Privacy Authority (DPA) concluded:

> As to the current practice in respect of intercepting and recording confidential telecommunications with a lawyer or other provider of legal assistance, the DPA has reached the opinion that this is unlawful. It follows from the recent legislative history, in line with the case-law on this issue, that the interests in the protection of these confidential communications prevails over the interests in finding the truth in criminal cases, also when it concerns the exercise of special powers of investigation. The systematic interception, recording and becoming acquainted with these confidential communications by the police and the public prosecution department is a breach of that.

The DPA formulated the four recommendations:

> 1. Lawyers have to ensure that there is clarity about their capacity and confidentiality towards the client when participating in telecommunications.
>
> 2. The public prosecution department has to prescribe a number recognition system to select conversations in which lawyers participate exclusively in their professional capacity.
>
> 3. The public prosecution department must secure that destroyed conversations should no longer be accessible, there has to be an obligation to, and procedure of destruction within the tapping system.
>
> 4. The public prosecution department must make further agreements with the police force managers (korpsbeheerders) who are responsible for the actual implementation of the obligation of destruction on base of a new Instruction.[345]

[344] ECtHR 24 November 2004, *Aalmoes & others v. The Netherlands* [2004], App. No. 16269/02, para. 7/8.
[345] Ibid [11].

The case caused an uproar amongst lawyers who feared risks of secret use of private information and inequality in proceedings. [346]

These risks did not alarm the Minister of Justice enough. Via letter dated 29 September 2003, the Minister of Justice informed the DPA that he did not subscribe to the findings of the DPA made in its report of 16 July 2003. The Minister considered that the practice of intercepting all conversations conducted via a tapped telephone number was not against the law. This include telephone conversations with a lawyer, with a subsequent control by the public prosecutor, whether or not any of these conversations fell with the scope of the privilege of non-disclosure enjoyed by lawyers. Consequently, the Minister would not follow the DPA recommendations.[347]

So the Applicants (Aalmoes and 123 other lawyers) complained before the ECtHR that the These rules did not comply with the requirement of foreseeability and do not offer sufficient protection against the arbitrary exercise of these powers or the unjustified breaches of their professional secrecy. Until 1 February 2000 only telecommunications could be intercepted in which a suspect was likely to participate. Under the new Decision and the Instruction, the police can take notice of privileged information and subsequently the public prosecutor who examines whether such information is privileged and, if so, orders its destruction. So both the police and the public prosecutor become aware of each confidential communication between a lawyer and a client that has been intercepted by means of an investigative power. Therefore, the regulations concerned do not guarantee the required level of protection and thus cannot be regarded as being 'in accordance with the law' or 'necessary in a democratic society' as the interferences which they entail are disproportionate.

The specification on foreseeability is therefore considered an important aspect of the principle of 'in accordance with the law' in addition to the fact that the expected level of privacy is not respected by damaging the trusted relation between lawyer and client as well the values of a democratic society as a whole. This last element is further specified in the next section.

4.4.10 'Necessary in a Democratic Society' in Proportional Balancing, Technology Related in 'Aalmoes'

The balancing of values to protect national security as is 'necessary in a democratic society' has a clear boundary in the abuse by governmental authorities. The problem lies in the grey area of what is deemed necessary under specific circumstances as, for instance, to fight terrorism including any actions in the preparation of possible society damaging activities. It is interesting to see that in this case it is stressed that technology (specifically telecommunications) is increasingly limiting the right to privacy and therefore must be used with the guarantees that take into account the 'state of the art' of the democracy.

In the *Aalmoes case* it was explained by the Court that it also considers that telecommunications, irrespective whether these are made from a private home or business

[346] *This means that there exist, in all the interception organisations examined, risks that may lead directly to accessing, altering or (non-)deletion of intercepted information or therewith connected meta-information (such as traffic data) ... by unauthorised third persons. In our opinion, such risks are to be addressed without delay*Ibid [4].

[347] He thought this to be in accordance with Article 126 AA CCP Ibid [12].

premises, are covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 (1). Therefore, interception, retention and subsequent use by domestic criminal investigation authorities of the contents of such communications amount to an interference with the right guaranteed by Article 8(1).
Also in this case the expression 'in accordance with the law' does not only imply the existence of a legal basis in domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of the interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power. Because of this the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to such secret measures.[348]

In this case the Court stressed the exception of the professional group of lawyers to protect their clients against unlawful intrusions within an impartial system of justice.[349]
Furthermore, according to the case-law of the Dutch Supreme Court under Article 218 of the CCP, an investigating judge may not authorize the tapping of the telecommunications made by a lawyer in his or her professional capacity, unless it is the lawyer who is the suspect of the offence under investigation. We also find this conclusion in the Financial Action Task Force (FATF) recommendations and the fourth Anti-Money Laundering directive that will be discussed in Chapter 6.
Given the sensitive nature of the relationship between the lawyer and their client, a very precise framework of regulations must be present to be acceptable. Taking all of this into consideration, the Court decided that The Netherlands regulations governing the interception of telecommunications in the context of criminal investigations are sufficiently precise and comprehensive, and provide for adequate safeguards, to be considered as within the 'law' for the purposes of Article 8(2).
It further considers that the possibility to intercept telecommunications in the context of a criminal investigation pursues an aim that is legitimate under Article 8(2), namely the prevention of crime. It remains to be determined whether the procedures for supervising the interception of telecommunications in which a lawyer participates are such as to limit the 'interference' to what is 'necessary in a democratic society'. The Court recalls that 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.[350] Although this led to the non-admission of the applicants, this case exemplified what boundaries exist in the application of the limitations to Article 8.

This reasoning fits to the doctrine of inherent limitations justified by the fact that the limits of the freedoms, protected by the Conventions, are by themselves justifiable because of their application in different circumstances and to the position of various concerned persons, for instance detainees, military personnel etc. This doctrine was accepted by the Commission but

[348] Ibid [23] *(see also;* ECtHR 25 June 1997, *Halford v. the United Kingdom* [1997], App no. 20605/92*, Reports of Judgements and Decisions 1997-III, p. 1017, § 49;* and ECtHR 4 October 2000, *Khan v. the United Kingdom* [2000], App no. 35394/97, § 26).
[349] Ibid [25]: '*it is clearly in the general interest that any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion. It is for this reason that the lawyer-client relationship is, in principle, privileged'.* See ECtHR 20 June 2000, *Foxley v. the United Kingdom* [2000], App no. 33274/96, para. 43. (While finishing this text the Hague Court decided that The Netherlands Secret Service was not allowed to tap conversations between Lawyers and their clients if there had not been an impartial institution that has decided that this concerned a matter of endangering state security(1-7-2015) ECLI:NL:RBDHA:2015:7436
[350] See ECtHR 28 September 2000, *Messina v. Italy (no. 2)* [2000], App no. 25498/94, para. 65.

rejected by the Court. The Court stated that where express restrictions are mentioned in the Article, for example Article 8, this is meant to be enumerative. However, as discussed above, these exceptions are worded so generally that the discretion for authorities is undefined that an enumerative list of exemptions, even with the application of the mentioned principles, still gives ample room for interpretation. The question remains whether the same reasoning could be applied to persons that are under suspicion of preparing terrorist or other criminal activities.

Specifically in the case of the application of interception techniques, there is an increasing sensitivity toward the intrusion of the personal sphere. The point of measurement is to be found in the proportionality of the action with respect to what is considered to be acceptable in a democratic society.

In order for a measure to be deemed 'necessary in a democratic society', it must respond to a 'pressing social need.'[351] This involves the test of proportionality. If a measure has been adopted which infringes an individual's Convention right in some way, it will not be considered disproportionate if it is restricted in its application and effect, and is duly attended by safeguards in national law so that the individual is not subject to arbitrary treatment.[352]

An example of this could be the interception of the communication of a lawyer if the lawyer himself is suspect.[353] In this case for the Supreme Court of The Netherlands, in principle it is obligatory to destroy the information of interception if there is communication between *lawyers* and other providers of legal assistance. But also here this obligation is not absolute: In this case the finding of the truth in the investigation of the 'confident' and partners in suspicion, will prevail over the privilege of the secret holder. In that case though the public prosecutor has to inform and require the judgment of an authoritative Member of the professional group of the secret holder concerning the use of interception. In this case that concerned the Dean of the Lawyers Association.[354] The Advocate General in this case expressed the dissatisfaction in this ruling by stating that the preliminary white papers on the laws history do not refer to circumstances where the truth finding prevails over the legal professional privilege.

4.4.11 Margin of Appreciation

Depending on the aim pursued, the Court grants Signatory States certain leeway in adopting the measures it considers most appropriate to pursue that aim, within the context of a democratic society. In the area of public morals, for example, State authorities have been considered to be in a better position than the Court itself to determine restrictions on the sale of pornography[355] or the legal recognition of transsexuals.[356]

It was asserted by some commentators in the United Kingdom before incorporation of the Convention that the doctrine was simply an interpretative tool specific to the international supervision of human rights and had no place in domestic arrangements for the protection of human rights. Others argue that it is analogous to the doctrines of justifiability that limit domestic adjudication of policy matters or decisions relating to the allocation of scarce public

[351] ECtHR 26 April 1979, *Sunday Times v. UK* [1979] 2 EHRR 245.
[352] ECtHR 27 August 1997, *MS v. Sweden* [1997], App. No. 20837/92, 3 EHRR 248.

[355] ECtHR 7 December 1976, *Handyside v. UK* [1976] 1 EHRR 737.
[356] ECtHR 17 October 1986, *Rees v United Kingdom* [1986] 9 EHRR 56.

resources, and that the adoption of a margin of appreciation doctrine is merely a change in form rather than substance.[357]

4.4.12 Surveillance: is the Use of Covert Devices in Line with Democratic Society? Specific Case Law

Surveillance does, undoubtedly, have two faces. It can act to curtail rights through, for example, reinforcing divisions within society, or it can be a vital tool in preventing and detecting crime. For citizens to accept and consent to certain forms of surveillance, that is to say its positive face, the State should be accountable for its actions. It cannot be left with an unfettered discretion to determine why and where it carries out surveillance on, and on behalf of, its citizens, without some form of legal responsibility. The governors and the governed should be subject to the law.[358]

Although no specific recognition of the facts have been issued by formal authorities, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament issued a report in which it was stated that:

> Access to data stored and processed on computer facilities, including remote computing facilities (cloud computing), is carried out by various intelligence programmes, the most prominent one being the NSA PRISM programme and the underlying legal provisions in the FISA Act and the USA PATRIOT Act. Furthermore, at least US and UK embassies, consulates and military establishments in third countries, including in other Member States, host electromagnetic interception facilities directed at GSM interception, including on heads of State and government.[359]

Interest groups confirmed this, as Accesnow stated that The United States government's ongoing, indiscriminate surveillance of worldwide internet users, authorized by Executive Order 12333, PATRIOT Act Section 215, and FISA Amendments Act Section 702, is inconsistent with the rights enshrined in the ICCPR, including clear violations of the right to privacy under Article 17.[360]
Christofferson has remarked that first the scope of protection is delimited, and then the scope of prohibition is determined. The European Court of Human Rights though, firstly examined in cases as P.G. v. U.K, whether the interference was 'in accordance with the law'. As noted above, this criterion comprises two main requirements: that there has to be some basis in domestic law for the measure and that the quality of the law is such as to provide safeguards

---

[357] Such an approach has received the support of the House of Lords, in the words of Lord Hope in R v Director of Public Prosecutions, ex parte (1) Sofiane Kebeline (2) Ferine Boukemiche (3) Sofiane Souidi [1999] 3 WLR 175.
[358] N. Taylor, *State Surveillance and the Right to Privacy,* Centre for Criminal Justice Studies, Department of Law, University of Leeds, <http://www.surveillance-and-society.org/articles1/statesurv.pdf>.
[359] The existence of the Five Eyes agreement, also known as UK-USA Agreement, was already confirmed bythe European Parliament special report on the on the existence of a global system for the interception of private andcommercial communications (ECHELON interception system), A5-0264/2001, 11 July 2001. See also: NSA Press release, 24 June 2010: Declassified UKUSA Signals Intelligence Agreement Documents Available, http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml. In: Working document 3 on the relation between the surveillance practices in the EU and the US and the EU data protection provisions Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Claude Moraes Jan Philipp Albrecht (Co-author), p.2, note 3.
1 [360] **Shadow Report to Human Rights Committee on US Surveillance Policy**
https://www.accessnow.org/cms/assets/uploads/archive/docs/INT_CCPR_CSS_USA_16495_E.pdf

against arbitrariness. Its reasoning is that implied powers of the police is not enough. [361] More specified statutory or other express legal bases must be present to use intrusive techniques by the investigative authorities.[362] The interference is not 'in accordance with the law' as required by the second paragraph of Article 8, if there has been a violation of this provision. In these circumstances, an examination of the necessity of the interference is no longer required.

In the following sections the use of surveillance devices and applied technology is tested in line with the requirement of legitimate limitation of privacy.

The continuing development of technology results in more sophisticated and intrusive means to survey a person's life. Those means are increasingly applied in criminal investigation and surveillance against (perceived) threats and potential criminal behaviour. In several cases, the use of technology is seen as an extra opportunity for intrusion into one's personal life. This often, but not always involves a more balanced appreciation.[363] In the case *P.G and J.H. v. the U.K.*, the government (defendant*)* acknowledged that the use of a covert listening device interfered with the applicants' right to respect for their private life. [364]It is interesting that the Court states that: 'Private life is a broad term not susceptible to exhaustive definition'.[365] Certainly when considering concerns of national security, the circumstances of this case justify the limitation. Similarly, the measures could be justified on the grounds of endangering society. The U.K. submitted that it was justifiable under the second paragraph of Article 8 as being necessary in a democratic society, in the interests of public safety, for the prevention of crime and/or for the protection of the rights of others. In the Court's balancing they considered the severity of the crime under investigation and the fact that B. was regarded as being surveillance-conscious. This latter element of the accused being surveillance-conscious is peculiar but nevertheless meant that conventional forms of surveillance proved to be insufficient. By tapping the conversations, the authorities could prove that an armed robbery was being planned. Nevertheless, They (UK) recalled, however, that in *Khan v. the United Kingdom*,[366] the Court found that the Home Office Guidelines governing such devices did not satisfy the requirement

[361] ECtHR 25 December 2001 (final)*P.G. and J.H. v. U.K.* App. *no. 44787/98* para . 44.

[362] *P.G. v. U.K.* para .'*It recalls that the Government relied as the legal basis for the measure on the general powers of the police to store and gather evidence. While it may be permissible to rely on the implied powers of police officers to note evidence and collect and store exhibits for steps taken in the course of an investigation, it is trite law that specific statutory or other express legal authority is required for more invasive measures, whether searching private property or taking personal body samples. The Court has found that the lack of any express basis in law for the interception of telephone calls on public and private telephone systems and for using covert surveillance devices on private premises does not conform with the requirement of lawfulness (see Malone, Halford and Khan, all cited above). It considers that no material difference arises where the recording device is operated, without the knowledge or consent of the individual concerned, on police premises. The underlying principle that domestic law should provide protection against arbitrariness and abuse in the use of covert surveillance techniques applies equally in that situation.'*
. The Court notes that the Regulation of Investigatory Powers Act 2000 contains provisions concerning covert surveillance on police premises. However, at the relevant time, there existed no statutory system to regulate the use of covert listening devices by the police on their own premises.

[363] ECtHR 25 December 2001, *P.G. and J.H. v. The United Kingdom* [2001]**,** App. no. 44787/98. Also referred by Van Dijk & Van Hoof on p. 673, note 31 (6 February 2001).

[364] Paragraph 12. On 4 March a covert listening device was therefore installed in a sofa in B.'s flat before the Deputy Chief Constable had confirmed the authorisation in writing. Conversations between B. and others in B.'s living room were monitored and recorded until 15 March 1995.

[365] *P.G and J.H. v U.K.*, para. 56

[366] ECtHR 4 October 2000, *Khan v. the United Kingdom* [2000], App. no. 35394/97, paras 26-28.

of ‘in accordance with the law’ and recognised that the Court was liable to reach the same conclusion in the present case.[367]

A more general point of view on surveillance by foreign agencies was issued by the European Parliaments committee. Although no specific recognition of the facts have been issued by formal authorities, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament issued a report in which it was stated that:

Access to data stored and processed on computer facilities, including remote computing facilities (cloud computing), is carried out by various intelligence programmes, the most prominent one being the NSA PRISM programme and the underlying legal provisions in the FISA Act and the USA PATRIOT Act. Furthermore, at least US and UK embassies, consulates and military establishments in third countries, including in other Member States, host electromagnetic interception facilities directed at GSM interception, including on heads of State and government.[368]

4.4.13 The Existence of an Interference with Private Life by Technology

It is quite unique that the Court provided a notion of ‘private life’ in the *Uzun* case. It does not happen often that the Court explains how to perceive a ‘reasonable expectation of privacy’, specifically concerning the intrusion into private life by advanced surveillance technology.
In § 1-57 of the Uzun case the Court concludes that private life is a broad term not susceptible to exhaustive definition. The Court considers a number of elements relevant to a consideration of whether a person’s private life is concerned by measures effected outside a person’s home or private premises. On top of that a technological consideration is made:

> Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[369]

---

[367] Ibid [37-38]:. As there was no domestic law regulating the use of covert listening devices at the relevant time (see *Khan*, cited above, paras 26-28), the interference in this case was not ‘in accordance with the law’ as required by Article 8 § 2 of the Convention, and there has therefore been a violation of Article 8 in this regard. In the light of this conclusion, the Court is not required to determine whether the interference was, at the same time, ‘necessary in a democratic society’ for one of the aims enumerated in paragraph 2 of Article 8.
[368] The existence of the Five Eyes agreement, also known as UKUSA Agreement, was already confirmed by the European Parliament special report on the on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), A5-0264/2001, 11 July 2001. See also: NSA Press release, 24 June 2010: Declassified UKUSA Signals Intelligence Agreement Documents Available, http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml. In: Working document 3 on the relation between the surveillance practices in the EU and the US and the EU data protection provisions Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Claude Moraes Jan Philipp Albrecht (Co-author), p.2, note 3.
[369] See also ECtHR 4 May 2000, *Rotaru v. Romania* [2000], App no. 28341/95, §§ 43-44.

The Court has referred, in this context, to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual (...) respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1). This personal data may be defined as "any information relating to an identified or identifiable individual" (Article 2).[370] This entails that recordings and photographs fall within the definition of private life, even in public areas.
The Court concludes therefore that recording of the applicants' voices when being charged and when in their police cell constitutes an interference with their right to respect for private life within the meaning of Article 8(1) of the Convention.[371]

4.4.14 Data Retrieved Following Surveillance, View of the ECtHR

The Court has a rather wide range of opinions of the use of technologically advanced means of surveillance. In an overview of the internet case-law of the ECtHR, a series of more or less comparable cases are presented in a research report where data is retrieved by (more or less) secret surveillance.[372] Although it is recognized that safeguards have to be installed in this sensitive and most intrusive way of surveillance, no hard conclusions are drawn out of the case law. Rather, the Court concluded that because "a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it […][373] [t]he Court must therefore be satisfied that there are adequate and effective guarantees against abuse"[374]

It must be recognized that even the Court is hesitant in ruling negatively about national guarantees found in national laws. On top of that, it is recognized that the risks of the electronic

[370] See ECtHR 16 February 2000, *Amann v. Switzerland* [2000], App no. 27798/95, §§ 65-67.
[371] *P.G. v. U.K.* para. 57. Para.. In the case of photographs, the Commission previously had regard, for the purpose of delimiting the scope of protection afforded by Article 8 against arbitrary interference by public authorities, to whether the taking of the photographs amounted to an intrusion into the individual's privacy, whether the photographs related to private matters or public incidents and whether the material obtained was envisaged for a limited use or was likely to be made available to the general public (see *Friedl*, cited above, opinion of the Commission, p. 21, §§ 49-52). Where photographs were taken of an applicant at a public demonstration in a public place and retained by the police in a file, the Commission found no interference with private life, giving weight to the fact that the photograph was taken and retained as a record of the demonstration and no action had been taken to identify the persons photographed on that occasion by means of data processing (Ibid., §§ 51-52).
The Court's case-law has, on numerous occasions, found that the covert taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence. While it is generally the case that the recordings were made for the purpose of using the content of the conversations in some way, the Court is not persuaded that recordings taken for use as voice samples can be regarded as falling outside the scope of the protection afforded by Article 8. A permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data. Though it is true that when being charged the applicants answered formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion must still be regarded as concerning the processing of personal data about the applicants.
[372] Internet case-law of the European Court of human rights Council of Europe/European Court of Human Rights 2011.
[373] See ECtHR 6 September 1978, *Klass and others v. Federal Republic of Germany* [1978], §§ 49-50, Series A no. 28.
[374] Internet case-law of the European Court of human rights Council of Europe/European Court of Human Rights 2011, p. 8 also referring to *Uzun*.

society, and specifically the use of internet in electronic communication, ask for specific means to be used by investigating authorities. These means though, have to be defined as precisely as possible.

In the report on the Courts decisions on internet of the Council of Europe[375] there is a concluding paragraph about the relevance of secret surveillance within the context of the Internet, and the so called ongoing evolution of Internet technology because the integration of the rapid development of equipment and techniques to monitor online communications are considered increasingly intrusive. Although not directly condemned as a danger or risk in the report it is registered that telecommunication companies each year provide large quantities of communications data to government agencies in response to lawful requests. They expect that the monitoring of internet use and telephone calls by national authorities could well be the focus of further litigation brought before the ECtHR in the future.

A clear and interesting example of all that can go wrong in delimiting the protection of personal sphere by 'secret surveillance', where all possible techniques were used, is found in the already mentioned case *Uzun v. Federal Republic of Germany.*[376] The measures that were taken and the absence of guarantees and control in the legislation as well as the 'blanket' definition in the applicable legislation made this case a clear violation of all principles that should be respected in a 'fair' limitation on basis of Article 8(2) ECHR.

Moreover, the term 'other special technical means intended for the purpose of surveillance' contained in the legislation, was not sufficiently clear and, having regard to possible technical developments in the future, its content was not foreseeable for the persons possibly concerned.[377] The text of the law had such wide coverage that all techniques on any one in the suspect's vicinity could have been subject to the operation of the 'secret surveillance.'

Consequently the Court draws the boundaries when the opportunity of surveillance are too broad and are not well-defined. The relevant aspect of 'defined by law' is not clear or foreseeable when it is not known what range of devices can be used for surveillance or under what circumstances these devices are allowed.

This had likewise been implicitly confirmed by the Federal Constitutional Court which had found that there was a risk of infringements upon fundamental rights by the use of new forensic techniques and that the legislator had to safeguard the respect of those rights, if necessary, by additional legislative provisions. Moreover, the applicant in this case submitted that the legal

---

[375] Ibid.

[376] ECtHR 2 December 2010, *Uzun v. Germany*, App no. 35623/05.

[377] Para. 29 of the decision: Article 100c § 1 no. 1 was inserted into the Code of Criminal Procedure by the Act on the fight against drug trafficking and other forms of organised crime (Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität) of 15 July 1992. The relevant parts of Article 100c of the Code of Criminal Procedure, in its version in force at the relevant time, provided*:'(1) Without the knowledge of the person concerned no. 1 a) photographs may be taken and visual recordings be made, b) other special technical means intended for the purpose of surveillance may be used to investigate the facts of the case or to detect the perpetrator's whereabouts if the investigation concerns a criminal offence of considerable gravity and if other means of investigating the facts of the case or of detecting the perpetrator's whereabouts had less prospect of success or were more difficult, no. 2 private speech may be listened to and recorded using technical means ... (2) Measures pursuant to paragraph 1 may only be taken against the accused. ... Measures pursuant to paragraph 1 no. 1 (b) ... may be ordered against third persons only if it can be assumed, on the basis of specific facts, that they are in contact with or will contact the perpetrator and that the measure will make it possible to establish the facts or to determine the perpetrator's whereabouts and if other means would offer no prospect of success or would be considerably more difficult.'*

provisions, on the basis of which GPS surveillance had been ordered, had not satisfied the qualitative requirements developed in the Court's case-law on secret measures of surveillance.[378] In particular, there was no statutory limit on the duration of such surveillance. That at least can be considered disproportionate, if not unacceptable in a democratic society. Furthermore, in view of the intensity of the interference, the prosecution, as opposed to the investigating judge had not offered sufficient protection against arbitrariness. The applicant further took the view that the use of numerous further surveillance measures in addition to GPS surveillance had led to his total surveillance by the state authorities and had violated his rights under Article 8 in that the law did not contain sufficient safeguards against abuse, in particular because no order by an independent tribunal had been necessary to authorise and supervise the surveillance measures in their entirety. A subsequent judicial review of the surveillance measures alone had not afforded sufficient protection to the persons concerned. The review was carried out only if criminal proceedings were instituted and, following such a measure, if by that measure the prosecution had obtained evidence which it intended to use at the trial.[379] Concerning the use of 'State secrecy' protection, it is always challenging to specify and pinpoint *any* guarantee against misuse of technological devices.[380]

4.5 Concluding Remarks on the ECtHR Case Law

The question that was answered in this chapter was: *how does the European Court on Human Rights validate, in its case law, exceptions to privacy? And on what principles are the decisions based?*

More specifically, this chapter has explored how the Court applies, in its case law, exceptions to privacy for reasons of crime-fighting and national security.

There are several areas where the exceptions occur. Most clearly are the exceptions in the surveillance conducted by authorities to prevent crime and terrorism. The principles that rule the decisions by the ECtHR often coincide with the Siracusa principles but are more detailed, due to the specifics of the case. The case law of the ECtHR shows that it is not easy to define under what circumstances good faith (cf. Article 3l of the Vienna Convention) is executed in a just manner by authorities concerning the use of intrusive technologies. The Court considers competences inherent to the task carried out which include limitations insufficient by reason of the general unspecified character. These general competences open the way to 'function creep'. Competence based on the law within a democratic society has to provide for a qualitatively acceptable law, which provides safeguards against arbitrariness. The notion of necessity to intrude on privacy has to be ruled by fair balancing, taking all interests into account, be they public or private interests. Consequently the court draws the boundaries when the opportunities for surveillance and the use of technologies are too broad and not well defined.

---

[378] He refers, in particular, to the case of *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECtHR 2006-XI and to that of Association for European Integration and Human Rights and Ekimdzhievv. Bulgaria, no. 62540/00, 28 June 2007. See also: ECHR 26 July 2007, *Peev v. Bulgaria* [2007], no. 64209/01:
44. In the present case, the Government did not seek to argue that any provisions had existed at the relevant time, either in general domestic law or in the governing instruments of the Prosecutor's Office, regulating the circumstances in which that office could, in its capacity as employer or otherwise, carry out searches in the offices of its employees outside the context of a criminal investigation. The interference was therefore not 'in accordance with the law', as required by Article 8 § 2.

[379] Ibid [44.].

[380] ECtHR 30 January 2008, *Ekimdzhiev v. Bulgaria* [2008], App no. 62540/00.

A key risk is the lack of control for the actual deployment of technology and competences, even when it is based on law. The relevant aspect of 'defined by law' is not clear or foreseeable when it is not clear what range of devices can be used for surveillance or under what circumstances these devices are allowed. This is stressed all the more when there is a risk of infringements on fundamental rights by the use of new forensic techniques and when the legislator has to safeguard the respect for those rights, if necessary, by additional legislative provisions.
Finally, and significantly, a very important conclusion of the Court is affirmed:

> *The first paragraph of Article 8 ECHR must be interpreted widely, the second paragraph has to be interpreted narrowly.*

This is stressed moreover with the increasing use of intrusive techniques in the telecommunication sector, as will be explained in the next chapter.

5 Telecommunication Law and Limitations on Privacy

5.1 Limitation of the Escape Route for Investigative and National Intelligence Authorities?

In Article 8(2) ECHR, the 'normal' protection of personal data can be set aside in cases of protection against criminal activities and when national security is concerned.[381] Of course this could only be acceptable if the restrictions are legitimate, necessary, proportionate and acceptable in a democratic society.

The question that follows is: are electronically-based investigations, namely the use of personal data and other judicial coercive measures in the telecommunication field, in particular interception of communications and retention of telecommunication data, compatible with the fundamental right of data protection and privacy?

Limitations on privacy, based on Article 8(2) often concern the use of interceptive techniques to obtain electronic or telecommunication data, including all electronic communication data obtained by electronic devices. Therefore it is important, for this thesis, to investigate the specific telecommunication regulations that makes these interception and the obtainment of these (personal) data possible.

The review of the telecommunication regulatory package, the so-called 'civil rights' directive on telecommunications, warns the participants, especially governmental authorities, that the development of identity-related techniques such as Radio Frequency Identification (RFID) asks for an increased responsibility to get access to the personal data that is the result of this technology. It demands further checks and verifications before access to such sensitive material may be granted.[382]

In these regulations we see a general spirit toward increasing the data protection and the wider protection of privacy as a whole on one side, and the increasing of data processing, including data transport on the other side. Additionally, there are increasing possibilities to limit the rights of the data subject if the circumstances require so. Europe remains attentive to the use of interception, the retention of traffic data and the legitimacy of the relevant regulations.

As telecommunication, or electronic communication, is considered to be both the most intrusive and the most vulnerable technology, the boundaries of data protection concerning the infrastructure and services for electronic communications are regulated. The Directive 2009/136/EC on privacy and electronic communications (the so-called 'e-privacy directive')

[381] Also stated in Article 52 of the EU Charter on fundamental rights the data protection directive in Article 13 and the proposal for a General PrivacyRegulation in Article 21 jo. 9,

[382] Consideration 56: Technological progress allows the development of new applications based on devices for data collection and identification, which could be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFIDs) use radio frequencies to capture data from uniquely identified tags which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens. To achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply.

requires an equivalent level of protection of fundamental rights and freedoms as in the general data protection directive. This regards, in particular, the right to privacy and the right to confidentiality with respect to the processing of personal data in the electronic communications sector. In the light of the purpose of the freedoms enshrined in the Charter of Fundamental Rights and Freedoms of the European Union, the directive also ensures the free movement of such data and of electronic communications equipment and services within the EU. This directive forms part of the 'Telecoms Package', consisting of a legislative framework designed to regulate the electronic communications sector.[383]

This e-privacy directive concerns the processing of personal data relating to the delivery of communications services. The directive is not considering any role of governmental agencies. Recital 51 Directive 2002/58/EC is somewhat of a fore-runner for the e-privacy directive above-mentioned proposal for a general privacy regulation that called for a more harmonized and stronger protection of the data subject.[384] This directive however concerns the service providers and gives national authorities a supervisory role. Nevertheless, this e-privacy directive lacks an amendment to the……..which allowed for a restriction of privacy on the basis of protecting public security, national security and defence.[385]
Although there does not appear to be a specific role for the service providers, there is an obligation for those providers to cooperate with national authorities, if need be, to intrude into the personal sphere of data subjects. In consideration (30) of the Directive 2002/22/EC (Universal Service Directive) it states that

> (…) there is no requirement for providers to monitor information transmitted over their networks or to bring legal proceedings against their customers on grounds of such information, (and) nor does it make providers liable for that information. Responsibility for punitive action or criminal prosecution is a matter for national law, respecting fundamental rights and freedoms, including the right to due process.

Providers are not legally obliged to monitor their data streams although they have to deliver traffic data on the basis of retention regulations as amended in Article 11 of the retention directive that is discussed later. In the amendments to the general telecommunication framework directive though, a stronger text is implemented to give

---

[383] The 'Telecoms Package' includes four other Directives on the general framework, access and interconnection, authorisation and licensing and the universal service. The 'Telecoms Package' was amended in December 2009 by the two Directives 'Better law-making' and 'Citizens' rights', as well as by the establishment of a body of European regulators for electronic communications (BEREC) DIRECTIVE 2009/140/EC OF THE EUROPEANPARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (*) <http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm>

[384] O.J. of the European Communities, 31 July 2002, L 201/37: This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

[385] (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights.

guarantees to ensure the compliance by national authorities of the Member States relating to their activities in the area of telecommunication networks and services with the ECHR.[386]

5.2 International Regulations that Provide for Limitation of Privacy Rights for Specific Purposes in Telecommunications

Specific purposes to limit privacy are mentioned quite often in the European as well as in the national privacy laws. Concerning the telecommunication sector in consideration 11 of the E-Privacy Directive, an unambiguous exposition is given for what purposes a suspension or intrusion of the privacy cf. Article 15 may be permitted.[387]

> (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.[388]

As referred to in Chapter 2, the European Convention is considered an integral part of the European Union legal framework. Regardless, a reference to this Convention is not included in the possibility to limit privacy as a sovereign right of the member states. The European subsidiarity principle, not to intrude upon the sovereignty of the Member States, is applicable to security issues.

---

[386] '3a.Measures taken by Member States regarding end-users access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law s, Directive 140/2009 (EC) of 18 December 2009 [2009], OJ L337/37.

[387] Maybe inspired by the fact that the concentration of the e-privacy directive was more internal market directed than privacy oriented: (8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered. 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) (*) as amended by Directive 2006/24/EC (**) and Directive 2009/136/EC (***) (unofficially consolidated version), consideration 8.

[388] 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), consideration 11.

For this paragraph I concentrate on the justifications of those 'necessary measures' in the telecommunications area for the protection of national and international security (and criminal activities that are connected with this threat). This applies to the majority of cases where limitation is permitted. Unsurprisingly, limitations to privacy may be permitted when cyberterrorism and the financing of such activities, falling under the umbrella of telecommunications, occur.

For the purposes of detecting, investigating and prosecuting criminal and security-endangering activities, data may be collected by authorities in using a range of electronic techniques as well as by less sophisticated interception of personal data. This takes the form of direct interceptions, such as using interception and listening devices, as well as less-direct methods like data mining public and private registrations. Although there may be grounds in criminal law for such investigatory measures, the remaining question concerns whether or not there are enough specifications and limits which are clear enough and provide guarantees against the arbitrary use of such measures.
Electronically-based intrusion into the personal private sphere is one of the ways governmental authorities acquire intelligence in national security processes as well as in criminal surveillance activities. Setting aside the 'spying or intelligence gathering' from one country to another in times of war, crises, or normal intelligence gathering as it is accepted in the international playing field, signal intelligence (sigint) and all other (electronic) communication intelligence (comint), this section considers the possibilities of electronic communication interception within the relevant(international) regulations. Although the case law reveals various degrees of acceptable intrusion, this section explores which interception techniques are available and utilised as well as what types of communications may legally be tapped. That those techniques are clearly intruding one's personal life was made clear in the earlier mentioned case *Uzun v. Germany* where almost any interception technique that was available to the Legal Enforcement Agency (LEA), was used.[389]
The term 'telecommunication' has changed, since the last update of the former regulatory framework in 2002, into 'electronic communication.' Electronic communication comprises all internet and social media communication as well as everything covered under telecommunication.[390] The broadening of the scope of electronic communication resulted in a strong inclination to start regulating the boundaries of data protection concerning the infrastructure and services for electronic communication, including internet in later versions of these regulative activities.[391]
The specific legal grounds and instruments in these restrictions are analysed below.

---

[390] Telecommunication in essence already comprises all: electronic transmission of signals over distances. This was not clear to everyone. This change should clarify the all encompassing application of the term.

[391] That is why Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 is amending the Directive 2002/58/EC on privacy and electronic communications. Within this E-Privacy Directive , 'protection' directive an unchanged exception is made for legal interception in a wide sense. Package: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (1) and Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services *Official Journal L 337*, 18 December 2009, pp. 0011 - 0036.

5.3 Interception, General Principles

The first time that the interception of telephone lines was accepted as a legal intrusion on privacy, notwithstanding other opinions,[392] was in the USA in the *Katz* case.[393] In the US and in Europe there has been an accepted policy that judicial authorities and police may obtain information via tapping or interception of telephone lines, although as of 2013 this policy has been under critical scrutiny. Already in 1967 the US Supreme Court decided in the Katz case that 'the reasonable expectation of privacy' did not extend to places, but only to persons in a certain place, in this case in a telephone booth).[394]

In the US as well in Europe there still is an ongoing demand by law enforcement agencies and intelligence agencies to increase the possibility to tap all kind of electronic communication. In the 2001 Convention on Cybercrime of the Council of Europe, obligatory demands were made under chapter 5, Articles 20 and 21, to intercept and store traffic data as well as content data, in national law. [395]

Before this Convention, beginning at the so-called Trevi[396] meeting in 1975 but strengthed in Maastricht 1991and increased by the 9/11 attacks and the 2004/5 bombings in London and Madrid, a considerable number of actions had already been taken to harmonise interception of electronic communications. [397] Firstly, because of the developments in the telecom sector, these actions were directed on fixed telephony and were later extended to mobile communications and the Internet. As described in the European Telecommunications Standardisation Institute (ETSI) [398] rules, lawful interception means legally-sanctioned official access to private

---

[392] Mr. Justice Harlan, concurring:
I join the opinion of the Court, which I read to hold only (a) that an enclosed telephone booth is an area where, like a home, *Weeks v. United States*, 232 U.S. 383, and unlike a field, *Hester v. United States*, 265 U.S. 57, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment, [p. 361] and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.

[393] Supreme Court 18 December 1967, *Katz v. United States*, 389 U.S. 347, see:
<http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZC1.html>.

[394] In the words of the Court: 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' Prior decisions indicate that that there is a twofold requirement: first that a person has exhibited an actual (subjective) expectation of privacy and; second, that theexpectation be one that society is prepared to recognize as 'reasonable.' Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected,' because no intention to keep them to himself has been exhibited. Likewise, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

[395] Convention on Cybercrime, Council of Europe, ETS-185, 1981,
<http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>.

[396] The name `Trevi' has been open to many interpretations. It has been variously attributed to: the presence at the 1971 meeting of the Dutch Minister Mr Fonteyn (which means fountain); the name of a famous fountain in Rome; the Trevi district in Rome;and as an acronym for either `Terrorisme radicalisme et violence' or terrorism, radicalism, extremism and international violence. ; Tony Bunyan, Trevi, Europol and the European state Statewatch;[http://www.statewatch.org/news/handbook-trevi.pdf]

[398] European Telecommunication Standardisation Institute:
<http://www.etsi.org/website/technologies/lawfulinterception.aspx>. The ETSI specifications are now in use in other countries that require the Lawful Interception of telecommunications.

communications. This allows a service provider or network operator to collect and provide law enforcement officials with intercepted communications of private individuals or organizations. Lawful interception (LI) implementation is required by the European Union International User Requirements 1995 which allows for LI to prevent crime, including fraud and terrorism. In the 1990s, voice transmission over the Internet became possible and law enforcement agencies (LEAs) consequently started to call for laws concerning interception within IP networks.[399] In the USA, network and service providers are required to cooperate with various law enforcement agencies under the Communications Assistance for Law Enforcement Act (CALEA).[400] In The Netherlands, the cooperation with investigative authorities in this respect is regulated under the Dutch Telecommunication Act, the criminal code and The Netherlands Intelligence and Security Services Act (NISSA). These standards have to be followed by telecommunication operators to ensure that interception is always possible. The problem is that these standards were all intended for interception of traditional fixed telephone lines (PSTN) and in the second instance, the mobile speech telephone connections. To be more precise as described in a technically oriented Article of the university of Brno:

The service is well implemented in traditional telephony (PSTN) within the telecommunication network infrastructure based on circuit switching. Internet is a packet based network and its communication proceeds on different layers of OSI model. Header information of a packet transmitted over internet can change as the packet moves from one network to another, especially on L2 and L3 layers. This makes LI and namely determination of the target identification a crucial issue. Comparing to traditional telephony, target identity cannot be precisely determined by single information from a data flow, but further data and their analysis is required.[401]

This means that data mining and profiling are techniques that will be increasingly used by law enforcement agencies and other investigative organisations. In the coming years it is to be expected that data streams of several networks and different functional sources, such as telecommunication, social networks, financial data and networks, RFID and other 'tagged' items, will be combined under the legal description of interception and analysis.

As mentioned, the Cybercrime Convention (CC) interception Article 20 (real-time collection of traffic data) and Article 21 (interception of content data) mandate that the concerned parties have domestic laws requiring service providers to cooperate in both the collection of traffic data and in providing the content of communications. This gives ample opportunities to both law enforcement agencies and national intelligence agencies to intercept, notwithstanding the guarantee for the protection of privacy and other human rights as given in Article 15 CC. In Recommendation N° R (87) 15 of the Council of Europe, regulating the use of personal data in the police sector (2002) Article 2.1 clearly states that the collection of personal data should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence.

Any exception to this provision is the subject of specific national legislation. The question is to what extent the collection and the use of personal data may be limited. For instance, there is

1. Official Journal C 329, 04 November 1996, p. 0001 - 0006 Council Resolution of 17 January 1995 on the lawful interception of telecommunications.

[399] ETSI introduced European recommendations for LI in ETSI TR 101 943.

[400] See: R. Polčák: *Structure and Proportionality of Fundamental Rights*, Masaryk University Journal of Law and Technology, Vol. 6: 3, 2012

still no distinction made between a clear criminal offense and criminal or security investigation and surveillance in more general matters connected to possible dangers. In the case of a clear criminal offence there is already a suspect. This is a narrower definition than general (criminal) investigation where no suspect is identified (yet).

One could agree with fewer guarantees against intrusion of privacy for the obvious suspect. In the latter case it is sufficient to use the procedural steps and other measures for tracing a criminal offender. For non-suspect (related) data, subject to any (computer) crime, it is not acceptable to lose all guarantees on data protection. This may take the form of people being innocent bystanders, who have nothing to do with the perceived crime and investigations whatsoever. Although this aspect is indicated in the proposed directive, this unlimited collection of data would be contrary to many privacy principles as stated in this study including that it is contrary to the purpose principle and that the action must be proportional to the purpose. This should not include the personal life of the innocent bystander. Procedures justifying the use of these intrusive techniques have to be clear and transparent and have to be evaluated by an independent authority. This should be provided by law in accordance with Article 9 of the Convention for the protection of individuals with regard to automatic processing of personal data.

It is not always made clear by judicial (or intelligence) authorities on what legal basis an investigation is taking place. Consequently, Internet Service Providers are not always immediately cooperative with these kinds of investigations as was made clear in 2006, in a case of the district court of California in the US referring to the starting of undefined 'data mining' and profiling without well-defined specific purpose.[402] :

The evolution of electronic interception is made clear in the case of *Uzun v. Germany*, considering the use of all available techniques for surveillance purposes. The Court found the use of GPS for surveillance and the consequential profiling of the whereabouts and the personal life of the subject a too far going intrusion in the personal life of a natural person.[403]
It must be mentioned and well understood, that the use of such intrusive techniques only can be accepted in a legal and moral sense if there are sufficient guarantees in these legal instruments on international and national level to protect the (innocent) natural person that is subjected to those interceptive and other data processing activities of the authorities.
Contemplating the necessity of interception, the Research and Documentation centre of The Netherlands concludes that the effective use of taps in conviction is relatively small and such taps may therefore be considered an intrusion upon the right on privacy.
The use of a telephone and Internet tap requires a definition of the categories of people who can be subjected to this investigative means, how long and with regard to which crimes this

[402]In this case it was stated that "[i]n the surveillance society, social sorting is endemic. In government and commerce large personal information databases are analysed and categorized to define target markets and risky populations. In the section on consumer surveillance we shall see how a company like Amazon.com uses sophisticated data mining techniques to profile customers, using both obvious and non-obvious relationships between data."(District Court California 3/17/2006.)

[403]*In the Court's view, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. Having regard to the principles established in its case-law, it nevertheless finds the above-mentioned factors sufficient to conclude that the applicant's observation via GPS, in the circumstances, and the processing and use of the data obtained thereby in the manner described above amounted to an interference with his private life as protected by Article 8 § 1.*
ECtHR 2 December 2010, *Uzun v. Germany*, App no. 35623/05.

investigation tool can be used, and which procedures should be observed while working up the tapped communication.[404]
A better specification of procedures and control of powers is crucial. This certainly was proven in the proven drama on telecommunication data retention rules.

5.3.1 Data Retention Laws and Regulations: Traffic Data and Location Data to be Retained for the Prevention of Crime and National Security

One of the most contradictionary measures that has been provided for by the legislators, is the obligation for providers of communication networks to retain data for the purposes of the prevention of crime and the protection of national security.
There are two main legal instruments on which this retention is based. Firstly, the implementation of the provisions on expedited preservation of stored computer data (Article 16) and secondly, the real-time collection of telecommunication traffic data (Article 18) in the Council of Europe Convention on Cybercrime[405] and the specification of these general obligations in the 'Data Retention Directive'.[406] The purpose of the retention directive is to harmonise Member States' provisions concerning the retention, of telecommunication data.

This section explains to which data and in what sense these regulations apply.

5.3.1.1 Traffic Data

Telecommunication service and network providers process different personal data for the purpose of transmitting communications, billing, interconnection, payments, marketing and certain other value-added services. Such processing involves data which indicate the source, destination, date, time, duration and type of communication, as well as users' communication equipment and, in the case of mobile telephony, data on the location of equipment.[407] This information is called 'telecommunication traffic data' for which it can be difficult to pinpoint a straightforward definition. For example, the Directive states that "Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof."[408] This same directive goes on to say that,

> [t]raffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection.

Further, a definition of traffic data is provided in Article 1(d) of the Convention on Cybercrime. The categories of data covered include: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Article 2 of the Retention Directive 2006/24/EC adds that "(a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user."

---

[404] WODC report 2012, p. 272.
[405] The '*Convention* on *Cybercrime*' (*ETS* 185) also known as the 'Budapest *Convention*'
[406] 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.
[407] As described on p. 2/3 of the evaluation document.
[408] Article 1, 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.

According to the European Commission:

Traffic data means data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication, including data relating to the routing, duration or time of a communication.[409]

Thus, with regard to the contents of traffic data, not being content data, there is hardly any aspect of the 'electronic communication traffic' data that will not include one of those definitions, extending to all identifying data derived by the processing over infrastructure or terminal equipment as long as it is not the content of the message itself. Even the headings of text messages are considered traffic data, which may easily correlate to the content of the message. Operators were obliged to store these data, not only for their own billing purposes but specifically for the use by police, intelligence services and other governmental agencies. This though, has significantly changed since the ruling of the ICJ on 8 April 2014 as will be explained later in this chapter, the essence of continued retention is still valid.

5.3.2 The Value of Traffic Data

It goes without saying that traffic data information is considered very valuable to be used by both law enforcement agencies and national security agencies for the prevention, investigation, detection, and prosecution of criminal offences.[410]
In the Cecile EU FP7 Report of 2012, a short historical background is given concerning the development of the traffic data hunger of police and other investigating authorities.

Demands for data retention can be traced back to the 'International Law Enforcement and Telecommunications Seminars' (ILETS) held at the FBI academy in Quantico, Virginia, which commenced in 1993 with the aim of developing global 'interception requirements' – standards for telephone-tapping by police and security agencies to be provided in all telephone networks. Following the first ILETS meeting, the very first EU Council of Justice and Home Affairs (JHA) Ministers adopted a Resolution in November 1993 – which was not published – calling on experts to compare the needs of the EU vis-à-vis the interception of telecommunications 'with those of the FBI'.[411]

In those meetings it was observed that the interesting traffic data was destroyed, by erasure, by the operators after a reasonable period of three months for handling the payment of the bills and possible technical purposes. This was considered a terrible waste of valuable data by the law enforcement authorities. Consequently the requirement for keeping the records on electronic communication data surfaced and resulted in obligations for the telecommunications and internet operators. These technical traffic data formed a very valuable addition to the already existing 'live' data from the use of 'tapped' data, including contents of the interception activities of all electronic communication sessions of suspects. The big difference was the fact that the traffic data were indiscriminately collected without any suspect or suspicion and are considered to be beyond a reasonable proportionality and purpose if one relates it to the aspect of investigation and prevention of crime.

---

[409] Opinion 15/2011 on the definition of consent Adopted on 13 July 2011.
[410] See also: Albrecht & Kilchling 2009, p. 7. and: Albrecht, Grafe & Kilchling 2008, p. 440.
[411] The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness <http://www.statewatch.org/news/2013/nov/Data-Retention-Directive-in-Europe-A-Case-Study.pdf>. A Project co-funded by the European Union within the 7th Framework Programme – Security theme, p.6.

Precisely this point was accentuated by Advocate General, Cruz Vilallon in prejudicial decision in December 2013 concerning the legality of the retention directive by the High Court of Ireland and the constitutional Court of Austria (Verfassungsgericht) in Austria and ultimately led to the destruction of the retention directive.[412]Both Courts wanted to have a prejudicial explanation of legality over the legal validity of the directive that, after all, allows a restriction of fundamental rights of the European Charter. This concerns, in particular, the provision in Article 7 and 8 of the Charter on the privacy and protection of personal data. The limitation of those fundamental rights under EU Treaty must be regulated proportionally (Article 5 (4) EUT and within the law (Article 52 (1) EU Charter).
The Advocate General, opined that this, particularly in view of the vulnerability of privacy in our 'surveillance' society, should include that the limitations of these fundamental rights should be sufficiently specified in the law. Given the messy definitions, the variation in terms of retention, the non-demarcated access for governmental agencies and the lack of adequate supervision, the Advocate General (AG) meant that the retention directive did not fulfil the requirements of valid legislation.

This did not mean, however, that this legislation should be pushed aside completely. After all, there are Member States, according to the AG, that were able to implement the retention rules within the framework of fundamental rights. Therefore, the European legislator should get a reasonable period of time to fix the errors. The European legislature, in particular the Commission was sensitively rapped over the knuckles by this opinion and the later annulment of the directive in the ruling of the Court though. The ruling and the opinion of the AG of course will have a severe impact on the way the new proposal will be finalized. It is not entirely inconceivable that the attention to the American NSA actions using PRISM and the activities of the British secret services using TEMPORA has strengthened the opinion of the AG and the ruling of the European Court of Justice in ruling the retention directive 2006 invalid on the 8th of April 2014.[413]

Although perhaps unsurprising, after the devastating opinion of the Advocate General, the Court ruled the directive invalid on 8 April 2014 on the grounds that it was insufficiently specified and there was no objective supervision. It does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter."

In addition to the lack of specified instruments and the extent to which they could interfere with the right to privacy, the aspect of independent control was lacking. Article 8(3) of the Charter requires that this independent control is governed by an independent authority to determine the compliance with the requirements of protection and security, which is not required in the directive.[414] The uncontrolled way the measures in the directive have to be applied and the fact that there is a reasonable risk for abuse (by the authorities themselves and third parties) results in the clear ruling of the court.

[412] Cases C-293/12 and C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland Ltd v. Minister for Communications* [2012], reference for a preliminary ruling on the validity of the data retention directive, by the Irish High Court (see here and here for a preparatory decision; on 27 January 2012); oral hearing on 9 July 2013 (see here); opinion of the advocate general on 12 December 2013 (see here at e-comm [in German]); judgment on 8 April 2014, <http://bit.ly/QL4tXj>.
[413] Digital rights Ireland and Seitlinger and others judgement of 8 April 2014. Joined cases C-293/12 and C-594/12 I-18.
[414] Idem, para 68.

Nevertheless, ruling that this directive is invalid does not mean that retention *in se* is illegal, although several member states courts also set aside the national laws based on the directive until a new directive appears. The retention of telecommunication data for the purpose of fighting serious crime and terrorism could still be conceived of as a legitimate measure.

Interestingly, at the same time as the issuance of the opinion of the AG in Europe on 17 December 2013, Judge Leon of the District Court for the District of Columbia in Washington declared the retention activities by the NSA unconstitutional in an unequivocal judgment. He considered concerning the undifferentiated collection of telecommunications data in violation of the fourth Amendment of the Constitution:

> I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every citizen for purposes of querying and analysing it without prior judicial approval. Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment.

He went on to say that "no Court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion."

It seems that now the judiciary are creating the limits to the infringements of privacy by security services and justice if the democratic control defaults instead of the legislature.
Although Judge Leon's ruling that daily searches on all citizens may not be agreeable, one must still determine the acceptable level of intrusion, within a democratic society. Since the case of *Klass v. Germany*[415] it was made clear, in a European Court of Human Rights perspective that telecommunication will fall under the protective ambit of Article 8[416] and is not easily discerned by relying on investigating activities by investigative requirements. In the next paragraph the influence of these legislative products on the personal space, as to be protected on basis of Article 8(1) ECHR, and the possible limitation of Article 8(2), as generally analysed in the preceding chapter, will be described in terms of the evaluation of the retention directive in 2012 and subsequent opinions and eventual ruling of the ECJ.

5.3.3 European Union, Directive 2006/24/EC Evaluation Report; an Illegal Directive [417]

The first legal activity on the EU level concerning the retention and use of data for law enforcement purposes was referred to for the first time in directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector.

[415] ECtHR 6 September 1978, *Klass and others v. Federal Republic of Germany* [1978], 2 EHRR 214. Also par. 4.5 for description of the case.
[416] *Klass* para. 41: Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of 'private life' and 'correspondence' referred to by this provision.
[417] 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, Official Journal of the European Union, 13 April 2006, L 105/54; Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC) Brussels, COM(2011) 225 final 18 April 2011.

This gave Member States the possibility to adopt legislative measures 'whenever deemed necessary' for the protection of public security, defence or public order, including the economic well-being of the State and for the enforcement of criminal law. Several Member States have adopted legislation providing for the retention of telecommunication traffic data as a result of the implementation of the EU directive. Requests for traffic data are increasing. Statistics provided by 19 Member States for either 2008 and/or 2009 indicate that, in the EU, over 2 million data requests were submitted each year, with significant variance between member States, from less than 100 per year (Cyprus) to over 1 million (Poland). According to information on the type of data requested, which was provided by twelve Member States for either 2008 or 2009, the most frequently requested type of data was related to mobile telephony.[418]

The use of the legislative measure has been under criticism, not only by 'privacy concerned parties' but also by the telecommunication operators, and other market players. The European Commission itself notes that by now there is a problem because the national provisions vary considerably. After the ruling of the ECJ the regulations are under more pressure to be very well defined. However, more obstacles have been created in light of the existing legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences. This is because service providers in the different member states are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention. The annulled directive attempted to harmonize these regulations and conditions but failed because of the space allocated for governments to apply their own definitions, authoritative competences (court orders or other official permissions) retention periods, and criminal acts that would provide for the use of the so-called retained data. One could say that it was not taken into account that the legality was not based on EU Charter on Fundamental Rights, and that the Directive, solely based on Article 95, is considered only fully legally acceptable if it is both 'necessary and genuinely meet(s) objectives of general interest. In the questionnaire that was sent out to the different stakeholders these doubts about the harmonization effects were confirmed by most participants.[419]

5.3.4 The Disputed Directive in EU Countries: In Perspective

The retention of telecommunication traffic data has been under discussion in several countries before the devastating ruling of the European Court of Justice and there have been several cases brought to national and international courts by individuals as well by states. From a historical perspective, it is very understandable that those countries with histories like the Second World War, such as Germany and Austria, as well as countries that have suffered under other totalitarian regimes, were not favourable toward the registration of these kind of personal data for possible investigative purposes. Before the European Court ruling in December 2008, the Bulgarian Administrative Court renounced the application of the directive;[420] in October 2009 the Constitutional Court of Romania[421] and in March 2010 the German Federal Constitutional

[418] The problems for LEAs and NSAs though, is that private networks and private lines are not subjected to these retention competence. Evaluation Report, p. 21.
[419] In September 2009, the Commission sent a questionnaire to stakeholders from these groups, to which it received around 70 replies. Responses have been published on the Commission website.
[420] Administrative Court of Bulgaria 11 December 2008 (decision no. 13627).
[421] Constitutional Court of Romania 8 October 2009 (decision no. 1258).

Court also ruled the directive inapplicable.[422] In June an action for annulment of a Data Retention Law was brought before the Constitutional Court of Austria.[423]

It is interesting that in the case Germany v. Commission not to implement the obligations of the retention directive action of infringement of EU obligations were issued.[424] After the decision of the German Constitutional Court, a formal complaint by the Commission was issued because of the lacking of the obligatory integration of the directive in national law. The Commission has withdrawn the action, but maintains the request for costs issued under proceedings.[425]

Following the lead of Germany, Romania and Bulgaria, the Czech Constitutional Court decided that the transposition of the Directive 2006/24/EC did not comply with the Czech constitution.[426] The Constitutional Court found that the data retention legislation infringes the information self-determination of an individual. The legislation furthermore did not fulfil the requirement of proportionality between the protection of the fundamental right to privacy and the investigation of crimes. The Court also criticized the vagueness of the delimitation of purpose for which the retained data should serve.

The debate continued in other member states. Ireland passed the Data Retention Act in 2012 whereas Sweden did not implement the directive at all in the first instance. It is understandable that Sweden, the first country in Europe to provide for an extensive data protection law in 1973, had serious hesitation to implement the directive.[427] According to the Swedish government, the implementation to the Swedish law is not necessary since the transposition would be contrary to the European Convention on Human Rights and the Charter of Fundamental Rights. Under heavy (financial) pressure by a ruling of the European Court of Justice though, the Swedish parliament passed a new data retention law in March 2012 that put Sweden in compliance with the European Directive 2006/24/EC.[428] One year before the Swedish law was passed, the Czech Constitutional Court adjudicated that a Czech law transposing the Directive contravened the Czech constitution.[429]

---

[422] Federal Constitutional Court of Germany 2 March 2010 (decision no. 1 BvR 256/08).
[423] AKVorrat.at: BürgerInnen klagen gegen die Vorratsdatenspeicherung, 15 June 2012. Available at: <http://akvorrat.at/node/61>.
[424] <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html>.
[425] Case C-329/12, 22 September 2012, *Commission v. Germany* [2012] ECR App: OJ C 287, p. 23.
[426] (even the the Hague Regional Court decided national retention law invalid: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:2498: mainly concentrating on the lack of safeguards: "*In that respect it is noted that a limitation of the data to be saved to the data of suspected citizens is not conceivable in view of the purpose of the Wbt, i.e. the effective detection of serious crime. In case of a first offender it is not possible to distinguish in advance between suspicious and non-suspicious citizens. The need for providing assurances and guarantees regarding access to these data, however, is all the greater because it is a very large interference, so that should be put to that high standard.*"(§3.8). Seealso: Fialová 2012.
[427] Be it that the state of Hessen in de FRG initiated the first data protection act in 1970.
[428] Case C-243/13, 10 February 2005, *European Commission v. Kingdom of Sweden* [2005] (2013/C 189/23) On May 30, 2013, after not complying to an earlier judgment of the Court of Justice (Case C-607/10 of the European Union held that Sweden failed to fulfill its obligations under EU law when it delayed complying with the Court's 2010 ruling regarding the country's implementation of the EU Data Retention Directive 2006/24/EC (the 'Data Retention Directive'). The Court ordered Sweden to pay a lump sum of EUR3,000,000. In the same judgment the Court Imposed a fine on the Republic of Estonia, for breaching the obligation to notify the measures transposing the directive, in accordance with Article 260(3) TFEU, a penalty payment of EUR 4224 a day from the date of the judgment of the Court of Justice.
[429] Constitutional Court of the Czech Republic 22 March 2011 (decision no. Pl.ÚS 24/10).

The Czech Constitutional Court was not the first to pronounce the Data Retention Directive unconstitutional. On the basis of the decisions, critics by privacy advocates as a reaction on the Evaluation Report, the European Commission prepared a review of the Data Retention Directive.[430] It is interesting to look into the reasoning of the Constitutional Court because they rely on the consideration of the proportionality principle to limit privacy. On 22 March 2011 the Czech Constitutional Court pronounced a judgement that held Czech data retention legislation, incompatible with articles 7, 10 and 13 of the Czech constitution.[431] These articles guarantee the right to privacy, protection of personal data and correspondence.

According to the Czech court, the provision failed to meet the requirements of proportionality between the public interest on the prevention of crime and protection of public order and the fundamental rights and freedoms guaranteed by the constitution. The principle of proportionality was assessed on the basis of three criteria: 1) the eligibility and appropriateness of fulfilling the purpose intended to protect another fundamental right or public interest; 2) selection of the means, that are the most considerate of the fundamental right; and 3) the prejudice to another fundamental right which must not be disproportionate in relation to the intended purpose.
The legislation, according to the decision, did not correspond with the degree of infringement of an individual's privacy and information self-determination. Therefore the massive retention of data pursuant to the ECA was not proportional in respect of the fundamental rights guaranteed by the Czech constitution, in spite of the fact that the storage of content of the communication was not permitted. The monitoring allows, according the court, the compiling of detailed information on social or political membership, as well as personal interests, inclinations or weaknesses of individual persons. Romania accepted the new retention law, based on the directive.[432] It is accepted that the retention applies to all data necessary to trace and identify the source of a communication. As a result of the ECJ ruling, the Romanian Constitutional Court (CCR) ruled in its decision no. 440 on 8 July 2014 that the second Romanian data retention law (no. 82/2012) was not constitutional.

In the Ireland case, although it already passed the Data Retention Act, Ireland argued before the EU Court of Justice that the retention directive was intruding upon national sovereignty and was contradictory to the subsidiarity principle. So the ECJ had to decide, on the basis of the subsidiarity principle, to distinguish between the areas within the competence of the member states of the European Community and those within the competence of the European Union. The Court decided that on basis of Article 95 EC, now 114 TFEU, to "adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."[433]

---

[430] European Commission: Proposal for a review of the Directive 2006/24/EC (Data Retention), no. 4, July 2011 <http://ec.europa.eu/governance/impact/planned_ia/docs/2011_home_006_data_retention_2012_en.pdf>.
[431] namely Section 97 paragraphs 3 and 4 of an Act nr. 127/2005 Coll. on Electronic Communication (hereafter: ECA),
[432] Law no. 82 from 13 June 2012: on the retention of data generated or processed by providers of public electronic communications networks and providers of publicly available electronic communications services, as well as on amending and supplementing Law no. 506/2004 on processing of personal data and life privacy in the electronic communications sector.
[433] See for a comparable discussion; S. Weatherill, 'The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a 'Drafting Guide'', *German Law Journal* 2011, Vol. 12, No. 3, p. 828-863.

This applies in particular where disparities exist between national rules, which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market, where the EU has the competence to regulate. Further, the Court finds it apparent that the differences between the various national rules, adopted on the retention of data relating to electronic communications, were liable to have a direct impact on the functioning of the internal market and that it was foreseeable that that impact would become more serious with the passage of time. Such a situation justified the EU Community legislature in pursuing the objective of safeguarding the proper functioning of the internal market through the adoption of harmonised rules.

The Court mainly concentrates on the aspect of the directive which concern the distortion of the market and the regulation of the activities of service providers without giving too much attention to the distortion of fundamental rights.
.[434] The June 2012 High Court of Ireland request for preliminary ruling to the ECJ with questions challenging the purpose declared by the Data Retention Directive, namely investigation, detection and prosecution of serious crimes and even the proper functioning of the internal market, has had a devastating result on the directive. The quintessence of the preliminary request was also if thispurpose could legitimize a limitation on the exercise of fundamental rights as provided for in within the specific meaning of Article 52(1) of the Charter of Fundamental Rights of the European Union.[435] Further questions posed by the Irish High Court related to compatibility with the right to privacy, the right to the protection of personal data the right to freedom of expression.[436]

The retention directive was intended to be adapted to the outcome of the evaluation report that had been produced. A new proposal was expected at the end of 2012, but is still 'under construction' in 2015[437] There have been several protests against a further extension of the 'blanket norm' as it is perceived by several Member states.[438] As of the opinion of advocate

[434] *Furthermore, Directive 2006/24 regulates operations which are independent of the implementation of any police and judicial cooperation in criminal matters. It harmonises neither the issue of access to data by the competent national law-enforcement authorities nor that relating to the use and exchange of those data between those authorities. Those matters, which fall, in principle, within the area covered by Title VI of the EU Treaty, have been excluded from the provisions of that directive. It follows that the substantive content of Directive 2006/24 is directed essentially at the activities of service providers in the relevant sector of the internal market, to the exclusion of State activities coming under Title VI of the EU Treaty. In light of that substantive content, it must be held that that directive relates predominantly to the functioning of the internal market* Case C-301/06, *Ireland v. European Parliament and Council of the European Union* [2009] ECR I-593. (Action for annulment – Directive 2006/24/EC – Retention of data generated or processed in connection with the provision of electronic communications services – Choice of legal basis)

[435] The limitation at issue takes the form of an obligation imposed on economic operators to collect and retain, for a specified time, a considerable amount of data generated or processed in connection with electronic communications effected by citizens throughout the territory of the European Union, with the objective of ensuring that such data are available for the purpose of the investigation and prosecution of serious criminal activities and ensuring the proper functioning of the internal market.

[436] E-comm: Update zu Vorratsdaten: Irland, Deutschland, Österreich - EuGH und VfGH. 18 June 2012. Available at <http://blog.lehofer.at/2012/06/update-zu-vorratsdaten-irland.html>.

[437] In accordance with Article 14 of the Directive, its application by Member States and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and statistics provided to the Commission, with a view to determining whether it is necessary to amend its provisions, in particular with regard to its data coverage and retention periods, Evaluation report, p

[438] Also comments on the hearing, initiated by the European Court of Justice on the 9th July 2013: The case, initiated by the Irish High Court (C-293/12 Digital Rights Ireland) and the Austrian Constitutional Court (C-594/12 Seitlinger and Others) invited commentary on the negative repercussions of the directive. One of the main arguments, according to EDRi, was that no evidence was available showing that the excessive collection of data is either necessary or proportionate in combatting organised crime and terrorism in the EU, while it can

general Cruz Villalón on the preliminary ruling on this case and the Austria case became public there came more clarity on the developing point of view towards the retention directive obligations.[439]

As in the first instance, the Advocate General gave his opinion on the question of whether it was constitutionally possible for the European Union to impose a limitation on the exercise of fundamental rights within the specific meaning of Article 52(1) of the Charter of Fundamental Rights of the European Union, by means of a directive and the national measures transposing it. He addressed the issues of the proportionality of Directive 2006/24 within the meaning of Article 5(4) TEU, the requirement, laid down in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be 'provided for by law' and if the directive observes the principle of proportionality, again within the meaning of Article 52(1) of the Charter.

The retention provisions are laid down in the Irish criminal Justice Act of 2005 (terrorist offences). Plaintiff states that the requirements of Articles 3, 4, and 6 of Directive 2006/24/EC incompatible with Article 5(4) TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims.

The Austrian retention obligations were laid down in the Telecommunication Act. Plaintiff, Seitlinger considers that the latter provision, which imposes upon his communication network operator the obligation to retain data without any reason, technical need or billing purpose and against his will, constitutes, inter alia, an infringement of Article 8 of the Charter. The ruling of the European Court of Justice has certainly confirmed this vision. The Austrian Data Protection Authority reported on 21 May 2014 that it has withdrawn the request for a preliminary ruling.

The evaluation report on the retention directive also examines the implications of the directive for fundamental rights, in view of the criticisms which have been levelled in general at data retention, and examines whether measures are needed to address concerns associated with the use of anonymous SIM cards for criminal purposes.[440] Retention of data on national and European databases is an issue which arguably will arise more frequently in the future before the ECtHR, given the proliferation of such databases.[441] At the European level one could cite SIS (the Schengen Information System), the CIS (Customs Information System), and VIS (Visa Information System) as likely domains for challenges. This is coupled with an increasing desire to share information and co-operate, together with increased concerns over security (following major terrorist attacks) and perceived immigration problems.[442].

---

be proven that data retained is used to investigate crimes not specified in the directive. Statistical data was provided by Austrian representatives demonstrating that between 1 April 2012 and 31 March 2013 the data retained was used in 326 cases, none of which involving terrorism. Alongside this, referring back to the decision made by the German Constitutional Court, it was argued that 'the cumulative effect of fundamental rights restrictions need to be taken into consideration', http://www.democraticunion.eu/2013/07/ecj-hearing-over-the-validity-of-the-data-retention-directive/>.

[439] Cases C-293/12 and Case C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources The Minister for Justice, Equality and Law Reform The Commissioner of Attorney the Garda Síochána Ireland and The General (*Request for a preliminary ruling from the High Court of Ireland) *and Kärntner Landesregierung Michael Seitlinger and Christof Tschohl* [2012].

[440] Council conclusions on combating the criminal misuse and anonymous use of electronic communications, 2908th Justice and Home Affairs Council meeting - Brussels, 27-28 November 2008.

[441] Evaluation report, p. 10.

[442] According to the European Data Protection Supervisor "the last decade also witnessed an increase in international police and judicial activities to fight terrorism and other forms of international organised crime,

A point that is failing in the evaluation report and in the ruling of the Court is that the directive is applicable to Telecommunication operators and internet service providers, but the fact is that there is a growing communication in closed and private networks as 'member communities' (including social networking sites and blogs) instead of the 'conventional' email. Further, it will be easy for persons with criminal intentions to use anonymous forms of electronic communication access by using Wi-Fi hotspots, pre-paid phones, and internet cafes. On top of that it will be difficult to register all mobile application mail programs (apps) such as Twitter, Skype and WhatsApp.[443]

5.3.5 Preservation or Retention of Telecommunication Data: What is the Difference?

Several sources have asserted that (from a privacy law perspective) it would be a better solution to strive for data 'preservation' instead of data retention.[444] The Commission, under pressure of the criticism on retention, commissioned a special research project to compare data retention and preservation techniques.[445] In this report a further description is given to the distinction of data preservation and data retention. Data *preservation*, also known as expedited preservation of stored data or 'quick freeze', refers to situations where a person or organisation (which may be a communications service provider or any physical or legal person who has the possession or control of the specified computer data) is required by a State authority to preserve specified data from loss or modification for a specific period of time (a maximum of 90 days under the Cybercrime Convention). A person or organisation may then be required, often by means of a court order, depending on the requestor, to disclose those data, usually on the ground that the data relate to specific individuals who are suspected to be connected to a particular criminal investigation or prosecution. The data may concern any type of stored information, including the content of communications (such as an email or voicemail message) as a well as non-content data such as 'traffic data' (that is, the route, time, destination and source of a communication). Data preservation therefore requires that data, which already exist in a stored form, are protected from external factors that would cause them to be deleted or their quality or condition to change or deteriorate. Preserved data or copies of those data may be accessed and used for legitimate purposes by authorised persons.

Unlike data preservation, data *retention* measures generally aim at requiring (some or all) operators to retain non-content data generated or processed as a result of activities of all users or operators' communications or network services so that they can be accessed by State authorities and used for 'public order' purposes when necessary and lawful. Data preservation

supported by an enormous exchange of information for law enforcement purposes." Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', Official Journal C 181, 22 June 2011, p. 1 - 23.

[443] This is also remarked by Ian Brown where he also refers to the fact that: Nielsen Online found in 2009 that these communities had overtaken e-mail to become the world's fourth most popular online sector after search, portals and PC software applications. They are frequently hosted on servers located in different jurisdictions to many of their members. Broadband, always-on Internet connections are now the default mode of access for home and business users in advanced economies. Users are increasingly switching from ISP e-mail services to messaging services hosted by companies such as Microsoft, Google and Yahoo. Ian brown, Communications Data Retention in an Evolving Internet, *International Journal of Law and Information Technology*, Oxford University Press 2010, Vol. 0 No. 0.

[444] See: Crump 2003, p. 191.

[445] Research study into evidence of potential impacts of options for revising the Data Retention Directive, November 2012, see also other documents on: <http://ec.europa.eu/dgs/home-affairs/what-we do/policies/police-cooperation/data-retention/index_en.htm>.

is a requirement according to the Cybercrime Convention and retention was required by the European directive. Therefore, the Member States that have ratified the Convention have the obligation to implement both measures.

As referred to in the 'shadow report,' Canada has announced plans to create a preservation order that would require telecommunication service providers to safeguard and not delete its data related to a specific communication or a subscriber when police believe the data will assist in a criminal investigation.[446] A preservation order is a 'quick-freeze' temporary order, and is only in effect for as long as it takes law enforcement to return with a search warrant or production order to obtain the data. Canada is keen to stress that this is not data retention for all individuals but only for specific investigations.[447]

In first instance there seems to be a preference, from the perspective of privacy protection, to support preservation described in the evaluation report:

> Data retention is distinct from data preservation (also known as 'quick freeze') under which operators served with a court order are obliged to retain data relating only to specific individuals suspected of criminal activity as from the date of the preservation order. Data preservation is one of the investigative tools envisaged and used by participating states under the Council of Europe Convention on Cybercrime.

Though it also has to be noted that Data preservation, as established in the Cybercrime Convention, has a broader scope in terms of the different types of data to be preserved. More specifically, Article 16 of the Convention refers to "specified computer data, including traffic data that has been stored by means of a computer system […]."

This is a clear indication that data preservation under the Cybercrime Convention is broader than the Data Retention Directive in terms of the purpose for which data may be required to be stored.[448] The Data Retention Directive requires operators to retain data for the purposes of the investigation, detection and the prosecution of serious crime as defined in national law (Article 1). According to Article 14 of the Cybercrime Convention, data may be preserved "for the purpose of specific criminal investigations or proceedings." This limits the application of the measures to an investigation in a specific case, but the types of crime for which data may be preserved are not specified. This though, is also the case in national legislation on the basis of the retention directive.

---

[446] European Digital Rights, Shadow evaluation report on the Data Retention Directive (2006/24/EC) 17 April 2011.

[447] *'This is not data retention. Contrary to what is the case in some countries, the amendments would not require custodians of data to collect and store data for a prescribed period of time for all subscribers, regardless of whether or not they are subject to an investigation. A preservation order would be restricted to the data that would assist in a specific investigation.* Shadow report, p. 8, referring to <http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32567.html>.

[448] To give some reference to the frequency of use in investigations at domestic level and in relation to partial disclosure (Articles 16 and 17 CC) I refer to the report:
With regard to the frequency of use of data preservation under Article 16 only four countries (two non-EU countries and two EU Member States) were able to provide estimates. The figures given differ significantly; three requests per year were indicated by one non-EU country, an estimated 100 requests in two EU Member States and 'thousands' of requests in one non-EU country. Three EU Member States stated that data preservation is never or only rarely used. Eight countries including seven EU Member States reported that no statistics were available, Final report, p.17.

The risk of function creep is that preservation concerns more case- and subject orientated activity to preserve traffic data for specific purposes in criminal cases that also apply to content data. Although it seems to fit in more properly with the thresholds of proportionality and purpose orientation, there are quite some doubts concerning their broad scope. The same vagueness, be it solely for traffic data, can be attributed to retention. The unmotivated retention order for all communication providers on the basis of an umbrella retention law for a much longer period, not specified for purpose or relevant suspects, is dangerous.[449] On a material basis though, only when there is a proportional, purpose-orientated and specified motivation for the preservation and use of data by the authorities for specified activities, concerning specified persons and necessary within the requirements of a democratic society, could such measures be allowed.[450] Preservation, when based on the Cybercrime Convention, is not very well-explicated and gives opportunity to include a range of criminal acts. The main difference with retention is that it should concern specified claims to a criminal act and as such would require that a court order also apply to content data. Retention is a general obligation for providers and will apply indiscriminately to any traffic data concerning electronic communication. It also applies for a much longer period. When actually required, authorities would need a court order in most cases although this varies among national legislations.
Still, there remains a growing worldwide uneasiness about retention. Although the United States is not subject of this study it is interesting to note that also here there is a growing concern about the retention of telecommunication data, partly based on the experience and the constitutional court decisions in the different European Member States.

For example, in the United States there has been a discrete proposal directed at countering child pornography, but striving for a far-reaching retention bill under almost false pretences, with a sneer to the EU directive by Marc Rotenberg, executive director of the Electronic Privacy Information Centre:
"But the data retention solution proposed in this bill is overly expansive and invasive. This collection of user data will, in fact, create a new threat for millions of internet users: the threat of dragnet law enforcement and data breaches. The experience with Europe is telling."[451]
Of course Rotenberg is referring to the hesitation, or outright refusal, of some Member States to transpose and implement the obligations of the retention directive already before the ruling of the ECJ.

Referring to this, Representative John Conyers, the Judiciary committee's senior Democrat, said his concern about the bill is that, although it's called the Protecting Children From Internet Pornographers Act of 2011, the mandatory logs could be used to prosecute all sorts of crimes, not only ones dealing with child safety. And the greater risk of this wide-reaching bill is that data logs could be accessed by State and local law enforcement and civil litigants in divorce or insurance cases as well.[452]

---

[449] This aspect of the retention regulation also withheld the German transposition of the directive in the German law. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345) (Eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter, wie sie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (ABl L 105 vom 13. April 2006, 54; im Folgenden: Richtlinie 2006/24/EG) vorsieht, ist mit Art. 10 GG nicht schlechthin unvereinbar; auf einen etwaigen Vorrang dieser Richtlinie kommt es daher nicht an).
[450] Materiell verfassungsgemäß sind die Eingriffe in das Telekommunikationsgeheimnis, wenn sie legitimen Gemeinwohlzwecken dienen und im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen (vgl. BVerfGE 100, 313 <359>), das heißt zur Erreichung der Zwecke geeignet, erforderlich und angemessen sind.
[451] Electronic Privacy Information Centre, <http://epic.org/>.
[452] Further information concerning situation USA: Law Enforcement Requests to Wireless Carriers Topped 1.3 Million in 2011. In response to recent >letters from Congressman Ed Markey (D-MA), nine mobile wireless

Also in this American case it is noted that the present form of preservation is considered a more acceptable form of the use of data if there is suspicion of criminal behaviour:

At the moment, Internet service providers typically discard any log file that's no longer required for business reasons such as network monitoring, fraud prevention, or billing disputes. Companies do, however, alter that general rule when contacted by police performing an investigation--a practice called data preservation.[453]

The most recently communicated cases show that the ECtHR as well as the ECJ are being faced with new concepts such as that of data portability and the right to be forgotten, in other words, the right for the data subject to object to the further processing of his/her personal data, and an obligation for the data controller to delete information as soon as it is no longer necessary for the purpose of the processing.[454] This will constitute a major inconsistency with the requirements based on the retention legislation. As stated in the so called 'Shadow evaluation report' by the European Digital Rights organization.[455] Several sources, including the aforementioned Member States find the retention directive an unnecessary and unprecedented violation of the fundamental rights of 500 million Europeans. This also includes the EFTA countries.
Norway, although not being a European Union Member State but obliged to integrate the directive on basis of the membership of EFTA, was also of the opinion that 'the data retention directive was a further step into a surveillance society.'[456] The ESA (EFTA Surveillance Authority) has reprimanded Norway about the way they implemented the directive.

5.4 Analysis of Problems as Considered in the Evaluation Report and Constitutional Court Decisions in the Member States

Although the ruling of the ECJ resulted in the invalidation of the directive it still is relevant to evaluate the deficiencies and complaints about this insufficient legal instrument for future directives and national regulations that will be expected to be in force when the dust of the annulment will be settled…

---

carriers have provided detailed reports of law enforcement requests for user cell phone records. These requests come from agencies - across all levels of government - seeking text messages, caller locations, and other information in the course of investigations. The reports show that companies turn over thousands of records a day in response to subpoenas, court orders, police emergencies, and other requests. The volume of requests has increased as much as 16 percent for some companies over the last five years, and some carriers have rejected as many as 15 percent of all requests that they found legally questionable or unjustified. EPIC recently filed amicus briefs in the Fifth Circuit and New Jersey Supreme Court arguing that disclosure of historical and real-time cell phone location information violates a reasonable expectation of privacy and thus requires a warrant under the Fourth Amendment. For more information, see EPIC: In re Historic Cell-Site Location Information, EPIC: *State v. Earls*.

[453] D. McCullagh, 'ISP data retention plan hits Capitol Hill snag', *CNET* 12 July 2011, <http://news.cnet.com/8301-31921_3-20078785-281/isp-data-retention-plan-hits-capitol-hill-snag/>.

[454] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - 'A comprehensive approach on personal data protection in the European Union', <http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_%282%29_15th_rt_2011.pdf>.

[455] European Digital Rights, Shadow evaluation report on the Data Retention Directive (2006/24/EC) 17 April 2011.

[456] Statement from the Data Inspectorate, July 2013, although the law was passed it was not enough: <http://theforeigner.no/pages/news/norway-opposition-fights-eu-data-retention-directive/>.

The main problem that countries have with the retention directive is the possible inconsistency with the common principles of personal data protection and especially the limitation of the privacy of the subjects that is the result of the ample possibility of the different Member States to apply the obligations set out in the directive. In this I will follow the inventory of the evaluation report.[457]

5.4.1 Purpose and Scope of Data Retention

As stated in the retention directive, the purpose and scope as such already gives rise to problems. For the use of retained data, it is very important to give a clear description when the retention laws are applicable and under what circumstances they are applicable. As the Article 29 Working party of European privacy regulators concluded in their opinion, "the directive does not seem to have been consistently implemented at domestic level. In particular it appears that it has been interpreted by Member States as if it was leaving open the decision on its scope."[458]
Besides the more principled problem of the intrusion of fundamental rights there also is the practical problem that among the Member States there is no harmonized limitation to the circumstances and pretences of when, where and by whom the data may be used. As described in the evaluation report in a more balanced wording, but ultimately with the same controversial content, it is emphasised that the inconsistency in the terminology and terms will create major problems in the actual national implementation of the directive:

> The Directive obliges Member States to adopt measures to ensure that data is retained and available for the purpose of investigating, detecting and prosecuting serious crime, as defined by each Member State in its national law. However, the purposes stated for the retention and/or access to data in domestic legislation continues to vary in the EU. Ten Member States (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, The Netherlands, and Finland) have defined 'serious crime', with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation. Eight Member States (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, and Slovenia) require data to be retained not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and for crime prevention, or on general grounds of national or State and/or public security. The legislation of four Member States (Cyprus, Malta, Portugal, and United Kingdom) refers to 'serious crime' or 'serious offence' without defining it.

Another inconsistency is of a statistical as well as of a more fundamental nature. The Commission has to be informed about the requests for retained data[459] on a yearly basis. The knowledge about the nature as well as of actual need and use of the retained data are not clear

[457] This section was written before the annulment ruling of the European Court of Justice of April 8 2014. Still the reasoning that also led to this ruling is still of general interest.
[458] Report 01/2010 on the second joint enforcement action: compliance at national level of telecom providers and isp's with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-privacy directive 2002/58/EC and the data retention directive 2006/24/EC amending the e-privacy directive, p. 1.
[459] Directive 2006/24/EC on data retention ('the DRD')1 requires Member States to provide the Commission on a yearly basis with statistics on data retention. Article 10 of the DRD states:
2006/24/EC *Article 10.(1) Member States shall ensure that the Commission is provide on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network.*

to begin with. According to the report concerning the statistics on the application of the data retention directive the different interpretation of the terminology will create many problems. This refers to the different interpretations to cases, the age of the cases and data, the difference in content of the data and differences in unsuccessful attempts to get data[460]

The problem of different interpretations of actions and interpretations of terminology by different member States as well as by different European institutions is not limited to statistical issues, but to a broader problem of interpretation of key terms in the retention legislation on national and international level as will be made clear in the next paragraph.

5.4.2 Data Retention Definitions

Relating to the definitions in the retention directive and the actual transposition into national laws, it has to be noted that there is no harmonized definition of the data to be retained, nor description as to how those data have to be reserved or protected. All such concerns fall within the competence of the Member States to decide upon procedures and security measures.

Moreover, the reasons for retention are not very well harmonized, in fact, they are not harmonized at all. For instance there is no definition in the directive of 'serious crime', nor is this definition to be found in the e-privacy directive where it is referring to the retention directive. The Netherlands' retention regulation is based upon the fact that the criminal act is considered a serious offence for which custody may be imposed and that investigation and prosecution of this activity is necessary.[461]

The definition of crime or serious crime varies among the member states as reason for the use of retained data. Reinhard Kreissl of the FP 7 project, IRISS, notes that even the media attention is influencing those definitions as well as the developing of the actual crimes. Hence, "[w]hen taking the notion of crime as a locally negotiated, socially defined and politically contested

[460]i. There are different interpretations of the term 'cases'. This term could mean (i) each and every item of data that was or was not provided, (ii) each request which may be for one set or multiple sets of data, or (iii) each investigation in which there might be multiple requests for multiple items of data.
ii. Where the request is addressed to a service provider is for more than one item of data, the data may be of different ages. Recording the age of individual data records could be unduly onerous for operators and/or competent authorities.
iii. Statistics submitted from some Member States only refer to requests for traffic and location data and not to subscriber information acquired from operators.
iv. The phrase 'Cases where requests for data could not be met' has been interpreted in various ways to mean i) cases where the service provider was unable to provide data that should have been retained under the DRD but were not retained; ii) data that were needed but which do not fall within the scope of the DRD, or iii) data that had been retained but were no longer available because the request was made after the expiry of the retention period Statistics on Requests for data under the Data Retention Directive, <http://ec.europa.eu/dgs/home affairs/what-we-do/policies/police-cooperation/data retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf>, p.2.

[461] In Article 126ng, CCP for any crime that can be punished with a sentence of 4 year detention and several crimes, mentioned in Article 67.
Article 126, Code of Criminal Procedure: concerning terrorism: Article 126zh:
1. In the event of indications of a terrorist crime the public prosecutor can, in the interest of the investigation, give an order to provide information on a user and the telecommunications traffic in respect of that user. See also: Van Kempen 2009, <http://www.ejcl.org/132/art132-1.pdf>.

concept as a starting point, crime waves should be understood as effects of mutually reinforcing public (media) attention, mirroring power relations and law enforcement activity." [462]

Even when the reason for retention is based on the investigation and detection or prosecution of 'serious crime', the actual contents and scope of this definition differs among Member States.[463] For instance, the description of serious offenses in The Netherlands differs from serious crimes in the United Kingdom. According to the evaluation report the purposes stated for the retention and/or access to data in domestic legislation continue to vary in the EU.

Ten Member States (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, The Netherlands, and Finland) have defined 'serious crime', with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation. Other Member states extend the use of retained data not just to serious crime but also to another range of criminal offences. Eight Member States (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, and Slovenia) require data to be retained not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and for crime prevention, or on general grounds of national or State and/or public security. The legislation of four Member States (Cyprus, Malta, Portugal, and United Kingdom) refers to 'serious crime' or 'serious offence' without clarifying what these differences entail.
In Poland the 'purpose' definition is not specified for 'serious crime' but generally: for prevention or detection of crimes, for prevention and detection of fiscal offences, for use by prosecutors and courts if relevant to the court proceedings pending, and for the purpose of the Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, Military Counter-intelligence Services and Military Intelligence Services to perform their tasks.[464]
In addition to the differences concerning the scope, definition and purpose of data retention, the addressee of these efforts is likewise varied.

5.4.3 The Addressed Operator and Access: a Definition of Data

Another deficiency is that countries differ in the obligations that exist for the operators which are defined in their national law. In some countries a differentiation is made between operators who are required to deliver the data on request by judicial authorities and those who are exempted from this obligation.[465] The United Kingdom and Finland exempt smaller operators from retention obligations based on consideration of costs. Several other countries have made arrangements to accept division of the cost by combined arrangements of cooperation or even outsourced retention activities to a specialized company. The Commission already noted that this could result in security problems which will require further research into this aspect.[466]

[462] Increasing Resilience in Surveillance Societies, To investigate societal effects of different surveillance practices from a multi-disciplinary social science and legal perspective.2012-2015, Deliverable D1.1: Surveillance, fighting crime and violence p. 158.
[463] See table 1, Purpose limitation for data retention stated in national laws, evaluation, p. 8.
[464] Article 180a, Telecommunications Law of 16 July 2004 as amended by Article 1, Act of 24 April 2009. See p. 8 Evaluation.
[465] The providers of publicly available electronic communications services or of public communications networks' (Article 1(1)).
[466] Evaluation, p. 9.

> Although in the evaluation the Commission referred to the fact that accordance with necessity and proportionality requirements, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted in the judgments of the ECtHR is applied, there are no concluding remarks to support this. And again the difference between Member states is cumbersome to the establishment of a harmonized way of access and securing the use of personal data. The report divulges that fourteen Member States list security or intelligence services or the military among the competent authorities. Six Member States list tax and/ or customs authorities, and three list border authorities. One Member State allows other public authorities to access the data if they are authorised for specific purposes under secondary legislation. Eleven Member States require judicial authorisation for each request for access to retained data. In three Member States judicial authorisation is required in most cases. Four other Member States require authorisation from a senior authority but not a judge. In two Member States, the only condition appears to be that the request is made writing.

The difference in access, procedures and competences seems to be very big. For example, in Poland the access to retained data is available to Police, border guards, tax inspectors, Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, military counter-intelligence services, military intelligence services, the courts and the public prosecutor.[467] Court orders are not necessary; requests in writing are sufficient. Other countries seem to have democratically reliable guarantees to use the retained data. For example, in Finland the data only are to be used for the purposes of investigating, solving and considering charges for criminal acts referred to in Chapter 5a(3)(1) of the Coercive Measures Act (450/1987). According to this Act a warrant is necessary although everyone can arrest this person on whom the warrant is issued.[468] In the UK it is still doubtful) in circumstances in which disclosure of the data is permitted or required by law, according to Article 7 of the Data Retention Regulations 2009.[469] Although in the overview it is stated that in The Netherlands the retained data are only accessible to the investigating police officer on the basis of a court order (by order of a prosecutor or an investigating judge), it has been shown in the Dutch law that the national general intelligence service and military intelligence will have access to these data when required. In The Netherlands all data is(was) accessible via the central Information point telecommunication Data (CIOT) and the additional information by the concerned operator on the basis of a decentralized regulation for the authorized Authorities.

5.4.4 Data Categories, Traffic and Location Data

In the annulled retention directive it was made clear that the scope of the data retention is traffic and location data and not content data. The definition in Article 2 of the directive further specifies this only to add related data to identify the subscriber or user. The user can be anyone connected to a telecommunication session. But the fact that any country has the competence within the ambit of the directive to further broaden or specify this, on the basis of the concept of the directive, results again in a patchwork blanket of defining location and traffic data.

---

[467] See annex.

468 See annex.

Section 1, Everyone shall also have the right to apprehend a person who, according to a warrant issued by an authority, is subject to arrest or detention.

[469] Data retention regulations 2009, <http://www.legislation.gov.uk/ukdsi/2009/9780111473894/regulation/7>.

Although in earlier proposals of the Commission reference was made to distinguish between telephone data and internet data for reasons of applying different periods of retaining the data, this did not reach the final proposal. It has been applied in several countries though, including The Netherlands, increasing the patchwork amongst European states.

The Article 29 Working Party of European privacy regulators concluded that several countries went beyond the defined provision for retaining specified traffic data. Too much data is retained, including content data![470]

Another point of interest is the extent of the technical scope; does the retention consider all attempts to call or just the successful connections? Does it apply to any terminal, including all kinds of terminal equipment?[471] Concerning the extension of data, some countries do not differentiate in kinds of data sessions, be it via telephone or via internet. Belgium for example only applies the retention to telephone data. The EU itself is not helpful in harmonizing the actual retention directive either. The European Parliament has asked for an extension to search engines in case of child pornography and sex offences. WP 29 stressed that it should be clear to have an enumerative list of categories to make explicit that no other 'obligation creep' was possible. All of these remarks are considering the same problem: an extended problem of deciding upon a harmonized, unambiguous application of a set of data and circumstances that would allow retention of a certain category of data.

5.4.5 Retention Period and Decisions of Constitutional Courts

Another problematic and readily discussed aspect of the directive is the retention period that is ordained by the respective member states' governmental authorities and specified in national law, sometimes after lengthy discussions about the period that may vary from six months to two years within conformity with the directive. The actual periods of retention even go beyond that as the Article 29 working Party of the European privacy regulators determined that some Member States retain data for up to ten years.[472]
Some of the Member States decided not to integrate the directive in the national legislation at all, as that has clearly happened in Germany after the decision of the Constitutional Court in March 2010.[473] The reasoning of the Constitutional Court is so interesting because the Court draws far-reaching conclusions to the consequences of retaining traffic data that go beyond the 'anonymous' qualification of traffic data but derive also content-related characteristic elements from the use and retention of traffic data. Therefore it is decided that the application of the retention directive and its integration in the national telecommunication law is declared void.[474]

---

[470] As to the internet traffic data several service providers were found to retain URL's of websites, headers of e-mail messages as well as recipients of e-mail messages in 'CC'- mode at the destination mail server. Regarding phone traffic data it was established that not only the location of the caller is retained at the start of the call, but that his location is being monitored continuously.Wording of the press release of 10 July 2010, on the report on the implementation of the data retention directive.

[471] See p. 12 -13 Evaluation.

[472] 'It showed that the directive has not been implemented in a harmonized way. Significant discrepancies were found between the member states, especially regarding the retention periods which vary from six months to up to ten years which largely exceeds the allowed maximum of 24 months.' Wording of the press release of 10 July 2010, on the report on the implementation of the data retention directive.

[473] Judgement of 2 March 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

[474] Paragraph 7: Voidness of the challenged provisions:
'The violation of the fundamental right to protection of the secrecy of telecommunications under Article 10.1 GG makes §§ 113a and 113b TKG void, as it does § 100g.1 sentence 1 StPO insofar as traffic data under §

The Romanian Constitutional Court in October 2009, in first instance[475] and the Czech Constitutional Court in March 2011[476] annulled the laws transposing the Directive into their respective jurisdictions on the basis that they were unconstitutional. The Romanian Court, in the line of the German Constitutional decision, accepted that interference with fundamental rights may be permitted where it respects certain rules, and provides adequate and sufficient safeguards to protect against potential arbitrary State action as was later confirmed in a new proposal. This was not enough though to accept the legality of the transposing law in first instance although after the ruling of the ECJ this legality was considered void anew. On the basis of the earlier case law of the ECtHR,[477] the Court concluded that the transposing law to be ambiguous in its scope and purpose with insufficient safeguards, and held that a 'continuous legal obligation' to retain all traffic data for six months was incompatible with the rights to privacy and freedom of expression in Article 8 of the European Convention on Human Rights resulting in the primary annulment. It was determined that the "individual citizen, therefore, had insufficient guarantees and safeguards against possible abuses of power by public authorities.[478]

5.4.6 The German Constitutional Court Case

Arguably the most interesting 'refusal case', even taking into consideration the annulment by the ECJ, was the decision of the German Federal Constitutional Court.[479] In this case the period of retention as well as the proportionality and legislative grounds for retention were contested by the complainants. This ruling is indicative of the doubts one can consider, including the creeping extension of diminishing privacy for public security purposes, and in this case the unlimited storage of telecommunication data for not specifically defined governmental use.

The English translation of the position of the complainants, initiated by a German lawyer, accentuates the disproportionality of the undifferentiated storage of (personal identifiable) telecommunication data.[480]

> The complainants are of the opinion that data retention above all infringes the secrecy of telecommunications and the right to informational self-determination. They regard the storage of all telecommunications connections without specific description of the occasion as disproportionate.
> They assert in particular that the stored data could be used to create personality profiles and track people's movements. One complainant, who offers an Internet anonymisation

113a TKG may be collected under this provision. The challenged norms are therefore to be declared void, their violation of fundamental rights having been established (see § 95.1 sentence 1 and § 95.3 sentence 1 of the Federal Constitutional Court Act (Bundesverfassungsgerichtsgesetz).'

[475] Romanian Constitutional Court, 8 October 2009 (Decision no. 1258), see evaluation p. 20.

[476] Judgement of the Czech Constitutional Court of 22 March on Act No. 127/2005 and Decree No. 485/2005; see in particular paragraphs 45-48, 50-51 and 56; see evaluation p. 20.

[477] *Rotaru v. Romania* (2000); *Sunday Times v. UK* (1979); and *Prince Hans-Adam of Liechtenstein v. Romania* (2001) ECtHR as cited above. Also p. 20 evaluation.

[478] Judgement of the Czech Constitutional Court of 22 March on Act No. 127/2005 and Decree No. 485/2005; see in particular paragraphs 45-48, 50-51 and 56.

[479] BVerfG, 1 BvR 256/08 vom 2 March 2010, Absatz-Nr. (1 - 345), <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html>.

[480] The constitutional complaints challenge §§ 113a, 113b of the Telecommunications Act (Telekommunikationsgesetz – TKG) and § 100g of the Code of Criminal Procedure (Strafprozessordnung – StPO) to the extent that the latter permits the collection of data stored pursuant to § 113a TKG. The provisions were introduced by the Act for the Amendment of Telecommunications Surveillance (Gesetz zur Neuregelung der Telekommunikationsüberwachung) of 21 December 2007.

> service, submits that the costs of the data storage disproportionately disadvantage the freedom of occupation of telecommunications service providers.[481]

The Court was not impressed by the commercial motive of the complaint.
The Court however does find the complaint admissible because of the limited applicability of the retention directive towards its purpose but also sees that retention as such is acceptable for different reasons and under different circumstances, which are legally sound:

> It's (the directives) provisions are essentially limited to the duty of storage and its extent, and do not govern access to the data or the use of the data by the Member States' authorities.
> With these contents, the Directive can be implemented in German law without violating the fundamental rights of the Basic Law.[482] The Basic Law does not prohibit such storage in all circumstances.

The German law was criticized on its disproportionate unspecified 'mining activity that is even beyond the obligations described in the retention directive.'

An important consideration in the objection to the transposed telecommunication law and the directive, is the massive, unspecified collection of data that is prescribed by the directive. The duty of storage essentially extends to all information that is necessary in order to reconstruct who communicated or attempted to communicate with whom, when, how long, and from where. This means that if authorities already know an IP address – for example from a criminal file or from their own investigations – they may demand information as to the user to whom this address was allocated. The legislature permits this for the purposes of the prosecution of criminal offences and regulatory offences and the warding off of danger, independently of more specific definitions. In such circumstances there is neither a requirement of judicial authority nor a duty of notification.

As stated in the introduction of this case, the aspect of deriving content-related characteristics from traffic data form an important consideration is made by the Constitutional Court, namely that traffic data may lead to content data and will form an intrusion in the personal life of a subject[483]

Of course this accounts also for other Member States and also for other areas as for instance the collection of data in case of license plates data (ANPR).

Under certain circumstances it is acceptable to retain data as a legal action because, under specified circumstances and of course taking into account the minimalisation principle towards

---

[481] <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html>.
[482] Supposedly the German Constitution (Grundgesetz)
[483] *In combination, the recipients, dates, time and place of telephone conversations, if they are observed over a long period of time, permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses.(…) . It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. In particular since the storage and use of data are not noticed, the storage of telecommunications traffic data without occasion is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas.*

the purpose of the activity, because sometimes the "reconstruction of telecommunications connections is of particular importance."

As stated by the Court specific tasks ask for specific competences. The problem though is, that the so-called strictly limited competences are not very well restricted in the case of national security and the activities of intelligence services.

5.4.6.1 Proportionality

Concerning the proportionality of legislative measure the German Constitutional Court concludes that there must be specific legal provisions in place.[484]

But the Court further specifies the requirements of proportionality and transparency:

> From this it follows for the prosecution of crimes that if the data are to be retrieved, there must at least be the suspicion of a criminal offence, based on specific facts, that is serious even in an individual case. Together with the obligation to store data, the legislature must provide an exhaustive list of the criminal offences that are to apply here.

So there has to be an understandable suspicion that could be reviewed as such based on facts. For warding off danger, it follows from the principle of proportionality that a retrieval of the telecommunications traffic data stored by way of precaution may only be permitted if there is a sufficiently evidenced concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federal Government or of a *Land* (State of the Federation) or to deter a common threat. It is interesting that the Court decides that these requirements apply in the same way to the use of the data by the intelligence services, since this is also a form of prevention of danger. This means, admittedly, that in many cases the intelligence services will probably not be able to use the data. However, to the Court this results from the nature of their tasks in advance intelligence and does not create a constitutionally acceptable occasion to relax the requirements for an encroachment of this kind that arises from the principle of proportionality.

More specifically, the Court has also underlined the special position of 'sensitive data' of persons and other legal persons. The Court considers that as a product of the principle of proportionality, it is constitutionally required that there should be a fundamental prohibition of transmission of data, at least for a narrowly defined group of telecommunications connections which rely on particular confidentiality. These might include, for example, connections to persons, authorities and organisations in the social or ecclesiastical fields which offer advice in situations of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staff are subject to other obligations of confidentiality in this respect.

5.4.6.2 Requirements of the Transparency of Data Transmission

In this case the Court also referred to the transparency aspect in a very specific manner. The Court ruled that the legislature must pass effective transparency provisions in order to

[484] In view of the particular weight of precautionary storage of telecommunications traffic data, such storage is compatible with Article 10.1 GG only if its formulation satisfies particular constitutional requirements. In this respect, there must be sufficiently sophisticated legislation with well-defined provisions on data security, in order to restrict the use of data, and for transparency and legal protection

counteract the diffuse sense of threat which may be conveyed to citizens by the storage and use of data which in itself is not perceptible. These provisions should include the principle that the collection and use of personal data should be open. With reference to the acceptable legitimate exception, the data may be constitutionally used without the knowledge of the person affected only if otherwise the purpose of the investigation served by the retrieval of data would be frustrated. This accounts for all investigative services, including the intelligence services. In contrast, in criminal prosecution there is also the possibility that data may be collected and used openly. There may only be a provision for secret use of the data here if such use is necessary and is ordered by a judge in the individual case. Insofar as the use of the data is secret, the legislature must provide for a duty of information, at least subsequently. This must guarantee that the persons to whom a request for data retrieval directly applied are in principle informed, at least subsequently. Exceptions to this rule require judicial supervision.

5.4.6.3 Purpose

Also the purpose definition in the legislature did not satisfy the Court, held against the requirements of the German Constitution:

> In this way it does not satisfy its responsibility for the constitutionally required limitation of the purposes of use. Instead, by giving the service providers a duty of precautionary storage of all telecommunications traffic data, at the same time combined with the release of these data to be used by the police and the intelligence services as part of virtually all their tasks, the Federal legislature creates a data pool open to manifold and unlimited uses to which – restricted only by broad objectives – recourse may be had, in each case on the basis of decisions of the Federal and Länder legislatures. The supply of such a data pool with an open purpose removes the necessary connection between storage and purpose of storage and is incompatible with the constitution.

The decision of the German Court as well as the ruling of the ECJ will certainly have a significant influence on several legislative products of the EU, ranging from retention to the general data protection framework. The fact that the German Court has severe doubts about the specification of the tasks and consequential competences of police and intelligence agencies supports the uneasiness that was presented in the evaluation report of the retention directive and the report of the Article 29 WP.
Taking these deliberations into consideration, it is quite a surprise that the European Commission of the EU, in the case of the transposition of the Retention directive was rather rigid in the enforcement of the compliance to the directive. Probably this was also taken into account by the ECJ in their final annihilation of the retention directive.

5.4.7 Further Action of the European Commission

Although there were several complaints about the necessity of the scope, purpose and effect of the retention directive and for a large part recognised in the evaluation report, the Commission still undertook actions against the Member States that did not comply with the obligation to transpose their legislation to the requirements of the retention directive. The European Court of Justice found the two countries (Sweden and Bulgaria) that did not transpose the directive in their national legislation were in violation with their obligations.[485] This is peculiar, considering the later annulment of the Directive.

[485] Case C-189/09 and Case C-185/09, respectively.

It might have been more sensible to wait with reprimanding and fining the Member States that have doubts about the directive until there is consensus about the new text of the directive. It would be wiser to view the directive in perspective with other legislation in development. I refer in that perspective to the aspect of non-specification of data, of different categories data subjects or users as now is foreseen in the concept for the retention of police data and harmonizing these specified categories for different periods in the data protection in criminal matters directive.[486] Clearly, the difference of treatment within the different Member States creates problems of inequality but also uncertainty for the data subjects. Likewise, there is uncertainty for the operators in terms of their obligations to data subjects.
On top of that it will also result in incertitude concerning the obligations for the operators. Also the aspect of location of retention and the border crossing may create problems and uncertainty.
It was also considered by the Commission to apply different storage periods for different categories of serious crimes, including terrorism. The actual practicability of such a differentiation is not considered.[487]
Probably this last reference is made to an earlier proposal of the Commission where the Commission made a distinction between the different types of data concerning the periods of retention for telephone data and internet data and different seriousness of crimes. [488] This is wording of the Commission in the evaluation is clearly referring to the proposal for a criminal data directive with diverging categories of data, connected to the categories of crime and the position of the data subject, which would be a better idea from the point of view of data protection.
It seems to be a mistake, that the legal committee of the European Parliament proposed to delete Article 5 j, that made this distinction in the concept Directive on the Protection of Personal Data by the Processing of Such Data by Criminal Justice Authorities since in their opinion, it is representative of an increase in bureaucracy and costs for the Member States and the legal effects have not been analysed. Even so, a promising qualification of data subject on the basis of their criminal or innocent status should not be set aside so easily.

5.4.7.1 Four Principles of Data Security

Because it is recognized in the directive that the retained data are of a highly sensitive nature, special attention in the evaluation is given to the handling of the data.
In Articles 7 and 9 of the directive, in line with the data protection directive, four principles of handling the data are obligatory:
(a) of the same quality and subject to the same security and protection as those

[486] COM(2012) 10 final.
[487]
'Whilst this diversity of approach is permitted by the Directive, it follows that the Directive provides only limited legal certainty and foreseeability across the EU for operators operating in more than one Member State and for citizens whose communications data may be stored in different Member States. Taking into consideration the growing internationalisation of data processing and outsourcing of data storage, options for further harmonising retention periods in the EU should be considered. With a view to meeting the proportionality principle, and in the light of light of quantitative and qualitative evidence of the value of retained data in Member States, and trends in communications and technologies and in crime and terrorism, the Commission will further consider applying different periods for different categories of data, for different categories of serious crimes or a combination of the two.'

[488] The Commission's proposal for a directive on data retention in 2005 provided for a retention period of one year for telephony data and six months for internet data. This strange proposal was actualy applied in the dutch retention law.

data on the [public communications] network;
(b) the data must be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
(c) subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and
(d) destroyed at the end of the period of retention, except those that have been accessed and preserved [for the purpose set down in the Directive].
In the oversight table of the evaluation it is made clear that even concerning those four principles there is no consistency between the Member States. In transposing the law into national law, several countries do not integrate the mentioned four principles in their national legislation. For instance Belgium, Spain, Estonia and Latvia do not address the principle of obligatory destruction of data the end of the period of retention.

5.4.7.2 Effectiveness

Concerning the proportionality and purpose orientation it also is important to note the reasons to retain the telecommunication data concerning the value of the data in individual criminal investigations. In the evaluation report this value is referred to in terms of effectiveness.
Member States generally reported data retention to be at least valuable, and in some cases indispensable. The numbers of requests and succeeded data integrated in criminal proceedings do not reflect the actual importance of using telecommunication data in actual convictions of criminal behaviour.

Also concerning the use of 'historic data' obtained on the basis of retention regulations, there is a stronger reliance in The Netherlands on the use of data than in other States and the data is used relatively easily for other purposes, which is also possible because of the broad scope of the police task and the definition of 'police data.' For example "the police's task is, in subordination to the competent authority and in accordance with the applicable rules of law to ensure the effective enforcement of the law and the provision of assistance to those who need it."[489] In addition, police data [means] any personal data that is processed in the context of the exercise of police duties."[490]

These data, retention data and all personal data concerning an investigation can be combined with data retrieved from any other data retrieval concerning the fulfilment of the police task. This, combined with the fact that The Netherlands is the country with relatively the highest rates of tapping-activities of telecommunications in the world, places The Netherlands investigative authorities in a rather obscure position.[491] Although the absolute number has not

[489] Article 3, Dutch Police Act 2012.
[490] Article 1a, Police Data Act.
[491] When the tapping statistics are compared to the total number of telephone numbers in use in The Netherlands, it turns out that annually, a tapping order has been issued for approximately one in every thousand telephones in use. The number of taps on landlines has remained stable throughout the years. The increase in the number of telephone taps since 1998 can be attributed mainly to the rise of mobile telephony. In 2010, the number of taps amounted to 22,006. In The Netherlands the number of taps has decreased over the last years, both in an absolute sense (with almost 17 per cent in 2010 in comparison to 2008) and in relation to the total number of telephone connections in use. For the year 2010, the number of Internet taps was published (1,704) for the first time; during the second half of 2010, investigators submitted requests for historic data pertaining to both historic traffic data and identifying data 24,012 times. An account is kept of the number of requests made of the CIOT as well. This number has steeply increased throughout the years. Regularly, the number of requests at the CIOT is criticized because the disclosure of identifying data of all kinds of people, connected to particular telephone numbers or IP addresses, means a violation of privacy. See Custers 2008.

increased substantially, the use of mobile tapping and certainly retained data is growing, not in the least by reason of the relatively easy way to acquire these data.

The data can only be acquired though, via the intermediary office, the Central Point for Telecommunication Information CIOT, but will be rather easily given, as stated in the citation.[492] But even then, the actual impact is small: The Netherlands reported that, from January to July 2010, historical traffic data was a decisive factor in just 24 court judgments. How decisive, under what terms or circumstances and if it was not possible to have a conviction without these data is not clear at all. Also the fact that there were more than 3000 criminal cases where tapped information was used, in that period points out the relativity of the 'decidedness'. There is no overview of the way the processing of these data took place. On the basis of Article 17 of the PDA all of these data can be provided to national and international police authorities and other national and international intelligence agencies, if it is necessary to fulfil the police task without much specified requirements.

5.4.7.3 Storage Period

Concerning the storage of (relevant) traffic data, there are problems regarding the principles of privacy protection as well as regarding the harmonization aspect. Although the statistical reference of the evaluation document is rather outdated, the principle is still valid. As stated in the evaluation document on the basis of statistical breakdown provided by nine Member States for 2008, around ninety percent of the data accessed by competent authorities that year were six months old or less and around seventy percent three months old or less when the (initial) request for access was made.[493] The question remains: if such a wide range of storage period is given in the directive, being six months to a period of two years, what period is actually needed. Does this reflect the proportionality and subsidiarity related to the purpose of data retention? It seems that a case and purpose specification on a more data-preservation orientated way is needed. I expect that the proposal for a new directive will harmonise this period.

To make the process of data retention more transparent for the citizens as well to the authorities that work with those data, a further harmonisation is needed. The fact that national legislation is substantially differentiated amongst the Member States makes it difficult to exchange data with the same statistical and proof value between competent investigating authorities. It would be a positive result of the evaluation to limit the actual storage period to a fixed term of six months, maybe with an extension to for instance a year under specific circumstances as motivated in national legislation, although even in this aspect a description, or at least an indication about these 'exceptional' extension and also access by differentiated authorities would improve the harmonisation of the retention legislation substantially. Also, from a privacy perspective, it would be a great improvement to set a clear limitation to the storage period in a secured area for an as short as possible term. As noted by several member states, it

[492] *Central Information Desk Telecommunication Research (CIOT)* Before a request for a tap is submitted, investigators need to make sure that the telephone number or IP address involved is still being used. This can be checked by asking the CIOT. The Central Information Desk Telecommunication Research is the link between investigative services and telecom companies and takes care of the storage and use of identifying data. Identifying data are the name, address and place of residence connected to telephone numbers, e-mail addresses and IP addresses. Providers of telephone and Internet services are obliged to refresh such data every 24 hours. Authorized investigative services can ask the CIOT for these data. Such requests may only be made on the basis of articles 126n, 126na, 126u, 126ua, 126zh, 126zi, 126ii Code of Criminal Procedure, Article 29 Intelligence and Security Services Act and Article 10.10 Telecommunication Act, in the context of a specific criminal investigation. WODC report 2012, p. 272.

[493] Evaluation report, p. 22 (see summary in Table 5 and further details in Annex).

also would be advisable to make a distinction amongst the access possibilities by competent authorities.

Concerning the actual evaluation document itself, it is remarkable that in the final comments on the evaluation the Dutch Senate concludes that the report does not adequately demonstrate the necessity and proportionality of the Directive (2006/46/EC) and that it fails to prove a 'pressing social need' for the Directive, as the E-Privacy Directive (2002/58/EC) already provides for storage of certain traffic data for billing and marketing purposes. The Senate also voiced reservations on its effectiveness. All these criteria – necessity, proportionality, pressing social need, effectiveness – have to be met in order to meet the safeguards of the European Convention on Human Rights (ECHR).

Doubts of the storage, quantity and period, were also raised in the referred opinion of the advocate general in the case of Austria and Ireland in the referred prejudicial question concerning the validity of the directive. This also concerns the collection of information known as 'big data' which are large collections of data in different databases. He considers this as a serious risk for the protection of individual citizens.[494]

5.4.8 Killing the Directive, the ECJ Ruling of April 8th, 2014

Although I already referred several times to the devastating ruling of the ECJ concerning the invalidity of the retention directive on the 8th of April, 2014, it is such a landmark case for this thesis that I have to give some specific attention to the ruling itself. The Court ruled the directive invalid because "by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data."

The Court ruled that the meaning of the directive is to harmonise the law among Member States, taking into account the privacy requirements;
It follows from Article 1 and recitals 4, 5, 7-11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions.[495]
In considering this, the Court took into account that retention directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the

[494] In his consideration under paragraph 72 he remarks as follows:
The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period.
[495] Cases C-293/12 and C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland v. Minister for Communications a.o.* [2012], I-18.

processing of personal data. [496] The question was if the requirements of article 8 of the Charter were met. [497]

Even in the critical stance towards the directive, the Court still is convinced that the purpose of directive and the limitation of privacy is legitimate and acceptable if the principles of limitation and the circumstances are taken into account:

So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 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 knowledge of the content of the electronic communications as such.

The Court is taking any intrusion on privacy as a serious matter, whether it concerns sensitive personal data or any action that will contravene the purpose of Article 7 of the Charter, even referring to the cases before the actual integration of the Charter by the Lisbon Treaty.[498]

Therefore there is no doubt in the mind of the Courts judges that the retention of data in itself represents an intrusion of the right to privacy.

> *As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.*

This interference is even strengthened by the fact that,(competent) authorities have almost unlimited) access to the personal (traffic) data that had to be retained by the providers.[499]

---

[496] *The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that Article and, therefore, necessarily has to satisfy the data protection requirements arising from that Article (Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 47).* Idem, I-19.

[497] *Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.*Idem, par. 30.

[498] *To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 75)* Idem, par. 33.

[499] *Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., Leander v. Sweden, 26 March 1987, § 48, Series A no 116; Rotaru v. Romania [GC], no. 28341/95, § 46, ECHR 2000-V; and Weber and Saravia v. Germany (dec.), no. 54934/00, § 79, ECHR 2006-XI).*

Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

*Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data*Idem, par. 35, 36, I-20.

The Court takes into account the fact that the fight against terrorism is important and as such presents the individual right to security next to liberty (privacy). The use of electronic data forms a necessary ingredient in this 'war':

> *It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest. The same is true of the fight against serious crime in order to ensure public. Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.*

But those instruments have to be proportionate to the purpose.[500]

Taking into account that the purpose is acceptable, the aspect of the proportionality of the used instruments, as in other cases mentioned, is of ultimate importance in the vision of the Court and should also be in the mind of the European legislator. The interferences upon the right to privacy have to be as limited as possible under the circumstances:[501]

> *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, 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.*[502]
>
> *Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.*[503]

Also here, following the opinion of the advocate general in the Austrian case, it is considered of the utmost importance to specify rules and circumstances and guarantees in a transparent way. Because the directive requires the retention of all electronic communication of all European citizens without exception by all member states, the Court states that "it therefore entails an interference with the fundamental rights of practically the entire European population.'[504] Moreover, it does not in any way discriminate with regard to the access of authorities nor does it specify the concerned offences that legitimise this access. Also the fact that no objective criteria are given to determine the access of authorities to the stored data.

---

[500] Idem, par. 46.

[501] *Where interferences with fundamental rights 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*Idem, par. 47. Interesting in this respect is the reference of the court to: *by analogy, as regards Article 8 of*
the ECHR, Eur. Court H.R., S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

[502] Idem, para 51.

[503] Idem, para 54.

[504] Idem, para, 56 e.f.

The fact that there is no limit specified to the means as well as to the application of the retention of *all* telecommunication data for *all* serious crime, makes the - also in the Marper case - mentioned proportional use of privacy-limiting measures, unacceptable and therefore invalid in a democratic society. The Court could have added to this that the national application even provides for law that applies to retention for all crimes, not even exclusively those considered to be serious. In addition, the retention period is wide-ranging without any objective criteria as to what should be retained and for how long.

> Finally then, the Court concluded that the directive is not specific, gives no clear and precise rules for the Member States to apply, gives no safeguards to the citizens and forms a serious risk of abuse and interference with the fundamental rights of the European citizens.[505]

In addition, the aspect of independent control as required in Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, is not required in the directive.[506] The uncontrolled way the measures in the directive have to be applied and the fact that there is a reasonable risk for abuse (by the authorities themselves and third parties) results in the clear ruling of the court.
On those grounds, the Court (Grand Chamber) hereby ruled the Directive invalid.
Importantly however, this does not mean that retention is necessarily illegal. The retention of telecommunication data for the purpose of fighting serious crime and terrorism is, for example, still a legitimate purpose.
The European legislator has to be very conscious of the principles of privacy concerning the proportionality of the measures in relation to the purpose the next time they propose the (new) retention directive.

5.5 Concluding Remarks Concerning Limiting Privacy in Electronic Communications by Retention, the Final Decision of the ECJ.

The limitation of the privacy of subjects by giving opportunities to police, prosecution officers and other potential LEAs to use any data that is to be retained by providers contributes to the insecurity of data subjects. If the competences and circumstances are not well defined by law,

[505] *It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.*
Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down Idem, para 66, 67.
[506] Idem, para 68.

privacy restrictions may apply to any natural person, ranging from suspects to completely innocent people.

The question raised at the beginning of this section concerning the compatibility of the fundamental right of data protection and privacy with judicially coercive measures in telecommunications for data collection and retention is largely answered by the case law of the ECtHR and the European Court of Justice.

National Courts, the ECtHR and the ECJ show, in their rulings, that the principles of proportionality, transparency, purpose specification and independent control should be guaranteed in the international legal instruments and national law based there upon.

The substantial meaning of the fundamental right may not be destroyed by unsubstantiated limitation. The more radical the limitation, the more specific the competences, means and circumstances of the limitation have to be defined in the law. This specifically applies to the technologically-advanced instruments of intrusion within the telecommunication sector.

It is not surprising that the retention directive has been the subject of constitutional court rulings and the subsequent ruling by the ECJ of its invalidity, by reason of its far reaching consequences for the personal life of the citizens of the EU and the increasing and undefined competences of prosecutors, police and other investigation services as the different national security agencies.

As we have seen, the principle of proportionality requires laws to be clearly defined, available and controllable as to the purpose and the subsidiarity principle. Most importantly though, as also referred to by constitutional courts, is the fact that there should be an objective control mechanism for agencies that are allowed to use the data without court orders or comparable legal requirements.

The scope of data retention is, in itself, questionable. The inability to control the competencies of the national authorities still continues to be a problem as we will see in the next chapter on anti-terrorism and anti-money laundering regulations.

According to EDRi (European Digital Rights) the initial retention directive was proposed as a result of lobbying by the British police on the UK government and was pushed through by the UK Presidency of the Council in the second half of 2005.[507] The European Parliament approved the Directive despite the viewpoint of the Civil Liberties Committee that the privacy of subjects would be heavily endangered by giving opportunities to police, prosecution officers and other potential LEA's to use any data that is to be retained by providers enhances the insecurity of data subjects if the competences and circumstances are not well defined by law.

Taking into account the EU Charter of Fundamental Rights and the European Convention on Human Rights, retention, as ground of a security measure that limits fundamental rights, must entail the principles of effectiveness, necessity and proportionality to the well-defined purpose should be considered to be fundamental in a new directive, as well as a procedure of independent (European) supervision. Nevertheless, the European Commission has not expressed a great willingness to take these principles into account. For example, European Commissioner Malmström responded to a German citizen by saying that "there is general

[507] EU Surveillance, The EDRi papers, p. 5.

support for the Directive and for data retention as a necessary measure for ensuring that certain Communications data are available for a limited amount of time for the investigation, detection and prosecution of serious crime."[508]

The Advocate General and the consecutive ruling of the ECJ made clear though, that the directive is insufficient from the perspective of harmonization as well from the perspective of safeguarding fundamental rights. In fact, it has been criticised as being "among the most controversial pieces of counter-terrorism legislation the EU has ever adopted and fierce debate as to its legitimacy and effectiveness has raged since the earliest stages of its drafting to the present day."[509]

This accounts for all intrusive electronic means that are used by investigative authorities. Legitimate rules should govern the use of those instruments, taking into account the principles that guarantee that legitimacy. The principle of retention for the fight against criminal and terroristic activities will be there to stay but must be specified. This should also account for the specification of purpose and procedures as well of the techniques that will be used. Until such a time that a new Retention Directive is adopted, LEAs and NIAs have substantial opportunities for interception under the Computer Crime Convention.

[508] Michael, 15 May 2013, *Frau Malmström und die 'Expertengruppe',* <http://blog.vorratsdatenspeicherung.de/2013/05/15/frau-malmstrom-und-die-expertengruppe/>.
[509] The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness
A Project co-funded by the European Union within the 7th Framework Programme – Security theme.

6 Anti-Terrorism and Anti-Money Laundering Regulations and Limitation of Privacy

6.1 Introduction

This chapter covers the development of anti-terrorism legislation and Anti-Money Laundering (AML) regulations from the perspective of the use of personal information by governmental authorities.

After the attacks and threats of terrorism against world safety in 2001 there was a fertile ground within the UN to legalise the subsequent 'war on terrorism'. Despite its global scope, the UN covers a worldwide gathering of different States and (legal) cultures that waters down the specification of legal rules and actions. Actions by the UN Security Council have had stern influence on further regulatory initiatives on terroristic threats, the financing of terrorist initiatives, and the money laundering making this possible. Comparable with the foregoing subjects in this thesis, the international regulations in this area do not excel in specification and transparency considering the possible limitation of privacy.

Globalisation of trade and communication, the development of the information society and the decrease of controls in trans-border data flows have increased the opportunities for money laundering and other financial transactions to support (international) terrorist and criminal activities.

In reaction to these developments, authorities aim to control those data and financial transactions and as a consequence fundamental rights as free flow of information, privacy and informational self-determination are progressively more restricted.

The question considered in this chapter is:

> Are the measures initiated by international governmental organisations and non-governmental fora to control and counter terrorist and other illegitimate activities, and their (financial) support in particular considering the anti-terrorism acts, and, counter-money laundering regulation and procedures, compatible with the fundamental right of data protection and privacy?

This chapter also relates to the diffusion of powers and influence of different organizations in policy development of anti-terrorism and anti-money laundering. Furthermore the legal instruments of the United Nations, Council of Europe and the European Union to counter terrorism and money laundering are reviewed in the light of the limitations on privacy. Anti-terrorism and anti-money laundering are strongly connected because of the use of laundered money for the financing of terrorist activities. This focus departs from the traditionally narrow attention paid to anti-money laundering efforts in light of the financing of the trade in drugs.

6.2 Anti-Terrorism and Anti-Money Laundering: an Introduction

It is often stated that terrorism would not survive without the illegal financing of those activities. Without money terrorists can neither function as an organisation nor can they

conduct attacks.[510] In an effort to counter these financing activities, a worldwide anti-money laundering framework had to be set up. Because of the inherently illegal and often informal financing network of terrorists, so-called Hawala networks, privacy intrusive measures seemed to be an effective method to survey these activities.[511] As Liliya Gelemerova (2011) stated, in her thesis on Money Laundering, the US was "the driving force behind anti-money laundering legislative developments, and the international community has sought to address these concerns and enforce global policies to fight money laundering.[512]

After the terrorist attacks of 9/11 and the bombings in London and Madrid, a boiling activity in the international theatre to set up committees and create new legislation arose to counter the perceived ongoing threat of terrorism. Those activities and regulatory actions are directed to two main areas:

1. measures to counter any terroristic activities, and
2. to counter any actions supporting terrorist activities, mainly concerning the financing of terrorist groups. The financially orientated counter measures are mainly covered by AML initiatives.

In several international regulations of different international organizations the limitations of fundamental rights are a 'condition sine qua non' to perceive the goal of the measures enacted in those regulations to fight terrorism. Because of the difficulty in countering terrorism and the financing thereof, governments agree too speedily and too often to rather undefined regulations and broad competences.

The main criticism and matter of concern is the use of rather vague definitions creeping into the criminal law and public law system. The 'perceived' crimes are defined in increasingly broad terms and they endanger legal certainty. Additionally, these definitions form the (criminal law) basis for limitations of fundamental rights, i.e. the right to protect one's personal life, by procedures as tapping and computer searches.
To shed some light on the development of this regulatory system, the development of anti-terrorism law will be described, followed by an analysis of AML regulations, which are closely connected to the anti-terrorist activities.

6.2.1 Definition of Terrorism

The fact that terrorism is politically and culturally sensitive makes it difficult to agree upon a harmonized definition on a worldwide basis, i.e. a description accepted by the United Nations. Basically, terrorism is not a legal term but due to the relevant regulations needs to be legally defined. As Rosalyn Higgins succinctly stated in her 2007 book, " 'terrorism is a term without

[510] Michael Freeman, ed., *Financing Terrorism,: case studies*, Ashgate Publishing, 2012, chapter 2, The estimated costs for '9-11'were between 350k-500k .

[511] Hawala networks in the Middle East and South Asia operate in the following manner: a worker in Dubai wants to send US $1,000 back to his wife in Pakistan. He finds a hawaladar and gives him the funds. The hawaladar contacts a fellow hawaladar (often an extended family member running a linked operation) in Pakistan. The hawaladar in Dubai gives both the worker in Dubai and the hawaladar in Pakistan a transaction code. The worker's wife goes to the hawaladar in Pakistan and gives him the code. If the codes match, the hawaladar in Pakistan gives his wife the rupee equivalent of US $1,000 minus a small fee. (Note that no funds have actually crossed borders.) *Terrorism Financing Methods: An Overview*, Michael Freeman and Moyara Ruehsen, Perspectives on Terrorism, Vol 7, No 4 (2013) [http://bit.ly/1FNsdMk]

[512] L. Gelemerova, *The anti-money laundering system in the context of globalisation: a panopticon built on quicksand?*, Nijmegen: Wolf Legal Publishers 2011, p. 3.

legal significance', it is merely a convenient way of alluding to activities of states or individuals widely disapproved and in which either the methods used are unlawful or the targets are protected or both." [513]

Higgins leaves her description inherently vague. Terrorism is a multi-interpretative concept that is politically influenced and is therefore described with reference to circumstances in the eye of the beholder: state, conqueror or victim.

An illustrative example is the fact that Yassar Arafat and Nelson Mandela have both been on the list of FBI terrorists and on the list of Nobel Prize winners for peace. Sadam Hussein used to be an ally of the U.S. until he became the most wanted terrorist.[514] Depending on time, culture and political conviction the terrorist for one, can be the freedom fighter to the other.

The FBI referred to terrorism in the Code of Federal Regulations as 'the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives' (28 C.F.R. Section 0.85).

The most specific description of terrorist behaviour in (global) international instruments has been stated in 2004. The United Nations Security Council Resolution 1566 condemned terrorist acts as:

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a State of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.

According to Kalliopi Koufa, the UN Special Rapporteur on Terrorism and Human Rights, 109 definitions were put forward between 1936 and 1981.[515] None of these proposals seemed to be acceptable. The 1972 ad hoc committee of the UN General Assembly also failed to agree on a definition of terrorism. This all is understandable because of the differences in the conception of terrorists and acts of terrorism and the status of national liberation movements. In the 1996 *ad hoc meeting to further develop General Assembly Resolution 51/210* an attempt was made to develop a non-binding definition but even this did not succeed. A clear definition is hardly possible in an international arena where there is a continuous change in loyalty towards each other. Even beyond the 9/11 initiated UN Security Council Resolutions 1368 and 1373[516] there still was no real unison to have a mutually accepted definition.

---

[513] Higgins 1997.
[514] The FBI started this list of 'most wanted terrorists' in the 1950. See also Conte, p. 8 referring to <http://www.fbi.gov/wanted/wanted_terrorists> and historical overview; <http://www.fbi.gov/about-us/history/brief-history>.
[515] Working Paper K K Koufa 26 June 1997, referred to by M. Muller QC, 'Terrorism, proscription and the right to resist in the age of conflict', *Denning Law Journal* 2008, Vol. 20, pp. 111-131, p. 113, http://bit.ly/1g7oooO>.
[516] Respectively adopted in Adopted 12 September 2001 and 28 September 2001.

Mark Muller refers to *Suresh v. Canada* (January 11, 2002).[517] The Supreme Court of Canada emphasized the risk of abuse in case a legal definition depends on essentially a political judgment. The Court says that "[o]ne searches in vain for an authoritative definition of 'terrorism'… [T]here is no single definition that is accepted internationally. The absence of an authoritative definition means that, at least at the margins, 'the term is open to politicized manipulation, conjecture and polemical interpretation. "However, the Canadian Court considered that the essence of the term 'terrorism,' as internationally understood, was reflected in Article 2(1) (b) of the International Convention for the Suppression of the Financing of Terrorism (UN General Assembly Resolution 54/109, 9 December 1999). This defines terrorism as any

> act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organisation to do or abstain from doing any act.

In the Court's view, this definition "catches the essence of what the world understands by 'terrorism'."

The Supreme Court interestingly noted that the broader the definition becomes, the greater the risk of arbitrary and 'manipulated' application. This certainly accounts for using these kind of descriptions in criminal law as we understand it.

Many observers believe the failure to agree on a definition since 9/11 has produced profoundly dangerous legal effects. This is because Security Council Resolution 1373 has effectively outsourced the definition of terrorism to member states to define 'terrorism' domestically without limitation. Muller refers to the slightly modified phrase that 'one man's terrorist is another man's freedom fighter' has been replaced with the dictum 'one State's terrorist is another State's freedom fighter.' These slightly modified words result in a drastically modified effect. Whether a person or group is terrorist in nature is no longer a matter of personal political opinion or of international debate but of national law as defined by the particular State or organisation, often a result of the political spur of the moment.[518]

If we look at the 'development' of the definition of 'terrorism' within the UN we see a reflection of the 'hot issues' in the global political arena and the need for governmental control. The ambiguity is clearly to combine actions of as many as possible Member States instead of creating a water tight offense description. Ben Saul worded this legislative failure of the Council as follows:

> ' (…) despite the lack of consistency in the identification of terrorist acts.(…) After September 2001, problems of definition became acute, since the Council adopted general legislative measures against terrorism—with serious legal consequences—without defining it. The Council has encouraged States to unilaterally define terrorism in national law, permitting wide and divergent definitions. In doing so, it illustrates how the Council has constructed an ad hoc working definition of 'terrorism' in its practice over time.'[519]

[517] Supreme Court (Canada) 11 January 2002, *Suresh v Canada*, [2002] 1 S.C.R. 3, 2002 SCC 1.
[518] Muller, p. 116.
[519] Saul 2005.

Kofi Anan proposed to develop a 'clear' definition that was clearly much too politically orientated so therefore never had a chance to be accepted:

> 'I endorse fully the High-level Panel's call for a definition of terrorism, which would make it clear that, in addition to actions already proscribed by existing conventions, any action constitutes terrorism if it is intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a Government or an international organization to do or abstain from doing any act.[520]

This is also clear to the coordinator of the proposed Comprehensive Convention on International Terrorism, Carlos Diaz-Paniagua who concluded that a definition of terrorism to be included in a criminal law treaty must have '*legal precision, certainty, and fair-labeling of the criminal conduct - all of which emanate from the basic human rights obligation to observe due process.*[521]

6.3 Character of United Nations Actions

Concerning the international activities to develop a framework against terrorism and connected activities, reference is needed to the discussions on this subject that have taken place in the global platform of the United Nations.

The United Nations is the platform where several worldwide measures have been proposed and accepted to address terrorist activities. Terrorism has been on the agenda of the UN and its predecessor, the League of Nations, since 1934, firstly in a draft convention for the prevention and punishment of terrorism. Although the Convention was adopted in 1937, it never entered into force, probably because of the growing popularity of the use of terrorism by its Members.[522] Since 1963, 14 different legal instruments and four amendments to prevent terrorist acts have been accepted and enforced by the UN Members States. Those instruments were developed under the auspices of the United Nations and its specialized agency, such the International Atomic Energy Agency (IAEA).

The initial countermeasures were mainly directed against drugs and organized crime activities. Since the 1990s the orientation on terrorism has shifted towards more globally organized and ideologically (including religious) based terrorist activities. The United Nations Global Counter-Terrorism Strategy in this sense was adopted by Member States on 8 September 2006 in the form of a resolution and an annexed Plan of Action (A/RES/60/288). This resolution and plan of action implies that all Security Council resolutions related to international terrorism should be implemented by the members. Therefore full cooperation with the counter-terrorism subsidiary bodies of the Security Council in the fulfilment of their tasks is required by implementing these resolutions by the Member States.[523]

It is interesting to see that those measures by the Council have shifted, based on the political climate at the global scale, i.e. the former existence and subsequent disappearance of the Cold

---

[520] United Nations General Assembly, *In larger freedom: towards development, security and human rights for all*, Report of the Secretary-General 2005, Chapter 3 para. 91.
[521] Barnidge 2007, p. 17.
[522] See for an overview: <http://www.un.org/en/terrorism/strategy-counter-terrorism.shtml>.
[523] See: <http://www.un.org/en/terrorism/strategy-counter-terrorism.shtml>.

War. According to Saul, the Security Council tried to avoid any political reference to acts of terrorism because they were afraid that in doings so, one of the parties in the 'cold war' would be offended, This might, according to Saul, have been changed after this period of antagonism between east and west subsided. Still there is and always has been a problem to declare and condemn certain deeds of aggression for instance in the Israeli/Palestinian conflict. This accounts for any act in a politically sensitive situation as also is the case in the "war like" situation in the Ukraine and the shooting of the civil aircraft of Malaysian airlines MH 17 on July 17th 2014.

> Until the 1990s, the Council was reluctant to regard terrorist acts as threats to peace and security, although this was attributable more to Cold War politics than to an absence of terrorist threats. Some of the most flagrant terrorist acts, such as the attack on Israeli athletes at the Munich Olympics in 1972 or the Air France flight hijacked to Entebbe in 1976,[524] failed to produce any action by the Council. In cases involving State violence against civilian aircraft,[525] and non-State aircraft hijacking and hostage-taking,[526] the Council treated such acts within the legal frameworks on the use of force and on international civil aviation, without reference to 'terrorism', allowing it to avoid the political and ideological disputes surrounding that term.[527]

Saul goes on to describe how the first Council resolution to use the term 'terrorism' was SC Res 579 of 1985 condemning 'all acts of hostage-taking and abduction' as 'manifestations of international terrorism'. Hostage-taking and abduction (and, implied by virtue, terrorism) were considered 'offences of grave concern to the international community', endangering human rights and friendly relations.[528] After the 2001 attacks and after the ending of the Cold War more than a decade before, the description and condemnation of 'terrorist attacks' did not much trouble the Security Council. Nevertheless a specific definition still was not created or, might not even been the intention of the Council. The meaning of those declarations and resolutions was to encourage the Member States to take measures against terrorist activities.

This specifically applies to the implementation of the counter-terrorist activities of the UN Security Council Resolutions 1267 and 1373[529] setting up the Council's Al Qaeda/Taliban

---

[524] Referring to Boyle 1982.
[525] Referring to: E.g., SC Ress 262 (1968) (Israel attacked Beirut airport); 616 (1988) (US destroyed an Iran Air flight; an ICJ action was discontinued after a settlement: Aerial Incident of 3 July 1988 (Iran v. US) (Order of Discontinuance), 22 February 1996); 1067 (1996) (Cuba shot down two civil aircraft).
[526] Referring to: SC Ress 286 (1970) (appealing for the release of hostages held in hijackings and calling on States to prevent hijackings); 337 (1993) (condemning Israel for forcibly diverting and seizing an Iraqi Airways aircraft from Lebanese air space.
[527] Saul 2005, para. III.
[528] Referring to: SC Res 579 (1985), paras 1 and 5; see also SC Pres Stat (9 October 1985). And 27 SC Res 579 (1985), preamble; see also Res 638 (1989), preamble.
[529] Resolution 13 73, S/RES/13773(2001) and Resolution1377 (2001)Adopted by the Security Council at its 4413th meeting, on 12 November 2001, <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/633/01/PDF/N0163301.pdf?OpenElement> and <http://www.unhcr.org/refworld/docid/3c4e94552a.html>. Following the adoption of resolution 1368 (2001), in the wake of the attacks of 11 September 2001, the Security Council adopted resolution 1373 (2001) which, *inter alia*, requires States to combat terrorism through a series of actions that are best carried out through the adoption of laws and regulations and the establishment of administrative structures. Resolution 1373 (2001) also called upon States to work together to prevent and suppress terrorist acts, including through increased cooperation. It also established the CTC to monitor implementation of the resolution by all States and to increase the capability of States to fight terrorism, see table: comparative table regarding the United Nations Security Council Committees Pursuant to Resolutions 1267(1999) & 1989 (2011), 1373 (2001) and 1540 (2004).

Sanctions Committee and the Counter-Terrorism Committee.[530] The committee has been very active in the creation and control of several legal instruments to counter terrorism:

> As a result of the attention focused on countering terrorism since the events of 11 September 2001 and the adoption of Security Council resolution 1373 (2001), which calls on States to become parties to these international legal instruments, the rate of adherence has increased: some two-thirds of UN Member States have either ratified or acceded to at least 10 of the16 instruments, and there is no longer any country that has neither signed nor become a party to at least one of them.

The Counter Terrorism Committee emerged out of this resolution and consists of all 15 Members of the Security Council. This committee was given the task to implement, stimulate and control the actions proposed in the resolution.[531] Comments of different groups and officials have indicated that the activities of these committees have severely damaged the position of the human rights. By decreasing the scope of these rights in stimulating authorities to limit those rights as privacy on behalf of anti-terrorism counter measures, the 'Trojan horse' is built into this fundamental right.

The contradiction is that in the actions against terrorism ther is hardly reference to the fundamental rights in the ICCPR and resolutions as General Assembly resolution 68/167 which provide for the reluctance to any interference in individual privacy rights. More specifically it is stated that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.[532]

Concerning the legitimate origin of the actions taken by the UN SC there also have been fundamental discussions on the actual legal question on whether, if the Security Council as a political organ, should be permitted to take legislative measures at all. In this respect it suffices to cite the words of Andrea Bianchi in the Oxford Journal of European Law:

> Accurate historical reconstructions of the preparatory works show how the SC as a political organ was merely meant to act as dispute settler under Chapter VI and as peace enforcer under Chapter VII.[533] The fact that Resolution 1373 lays down legal

[530] See: Foot 2007.

[531] The 9/11 terrorist attacks resulted in the passage of Security Council Resolution 1373 on 28 September 2001 under Chapter VII provisions, like 1267. This significant resolution 'imposed sweeping legal obligations on UN member states. It created an unprecedented campaign of nonmilitary, cooperative law enforcement measures to combat global terrorist threats.' Whether or not states were parties to other anti-terrorism conventions, they were required not only to freeze assets and deny terrorists safe haven, but also to 'update laws and to bring terrorists to justice, improve border security and control traffic in arms, cooperate and exchange information with other states concerning terrorists, and provide judicial assistance to other states in criminal proceedings related to terrorism.'14 The Counter-Terrorism Committee (CTC) is also a committee of all fifteen members of the Security Council and was set up to monitor state implementation of these obligations, primarily through state provision of reports on the legislative and executive actions they were undertaking. See Foot 2007, p. 494.

[532] United Nations A/RES/68/167 General Assembly Distr.: General 21 January 2014 Sixty-eighth session Resolution adopted by the General Assembly on 18 December 2013 [
on the report of the Third Committee (A/68/456/Add.2)] 68/167. The right to privacy in the digital age

[533] Bianchi 2007.

> obligations of a general character has caused many to characterize it as a form of 'legislation' on the part of the SC.[534]

In essence this statement also accounts for any Council resolutions: they do not create international law, but are normative obligations on Member States under the Charter.

6.3.1 Doubts about the Legitimacy of Measures

There has been an increasing suspicion amongst scholars and politicians about the 'trade off' between security and privacy. [535] Due to circumstances that are still valid in a large part of the world and particular priorities of the United States, the UK, France as the Middle East, Asia and Africa, there is increasing attention given to the threat of potential terroristic factions and their activities. As a consequence, support is given to legislative activities of the UN and SC to counter terrorism with little attention paid to privacy protection.[536] The legislative actions against terrorism have been largely justified with reference to necessity in the war against terror.

> As a former assistant to the White House Counsel Alberto Gonzales later put it in explaining the Bush administration's approach to countering terrorism, the war paradigm means that you are entitled to kill 'a suspected adversary across from you, you're entitled to kill that person with no due process or advance warning whatsoever . . . [even though] that is going to mean sometimes hurting innocents in the process.[537]

Because the actions of the UN Members may be based upon Resolution 1373, a reference to human rights is easily overseen. A general warning to include references to UN human rights conventions and more specifically privacy protection in this case would be highly advisable. Foot highlighted this deficiency with reference to Robert K. Goldman, appointed as the UN independent expert on the protection of human rights and fundamental freedoms while countering terrorism, who stated:
"that resolution [1373], regrettably, contained no comprehensive reference to the duty of States to respect human rights in the design and implementation of such counter-terrorism measures."[538]

In the resolution it was considered enough to just refer to a general situation of threatening the Global security. In the review of 2012 on the anti-terrorism policy, there were general references to human rights conventions and to the construction of a 'legal mandate.'

---

[534] Reference Bianchi note 12: In fact, the resolution seems to fit the definition given by Yemin: *'legislative acts have three essential characteristics: they are unilateral in form, they create or modify some element of a legal norm, and the legal norm in question is general in nature, that is, directed to indeterminate addressees and capable of repeated application in time'*: Yemin 1969.
[535] Solove 2011.
[536] Foot 2007, p. 500, Thus, it seems likely that Resolution 1373—largely framed by the United States and promoted as an act of solidarity with Washington—may have been deliberately designed to reflect the US preference for fighting the global war on terror unhindered by what it saw as inapplicable or outdated humanitarian laws. Human rights NGOs worked energetically to try to persuade Security Council members to include in the Resolution a paragraph which stated that governments had to make sure that their anti-terrorist actions were in compliance with international humanitarian and human rights law.
[537] Foot 2007, p. 501. *Promotion and Protection of Human Rights: Protection of human rights and fundamental freedoms while countering terrorism*, U.N. ESCOR, Comm'n on Hum. Rts., U.N. Doc. E/CN.4/2005/103 at 6, 21 (7 February 2005) prepared by Robert K. Goldman.
[538] Foot 2007, note 25 on p. 497.

Leaving the question of the legally binding status of the UN policies and mandates on its Member States, one can already agree on the fact that all actions of the UN general assembly, as well as the Security Council decisions based upon the GA resolutions, are directed at stimulating further cooperation between the Member States to counter terrorism. It is presented as a policy directive, leaving aside specific instructions as is comprehendible, given the sensitive character of prescribing rules concerning the act of terrorism.

Most measures and international legislation that form the basis for actions to counter terrorism are directed toward cooperation between member States as for instance is evident in resolution 94/60 where cooperation as well as the enactment of international legal instruments directed to the elimination of the act of terrorism is stressed.[539]
But it is also recognized by several Members that the activities in this area should not be used by authorities as an excuse to limit the privacy of the citizens by extending powers of investigating and other national authorities in an uncontrolled and limitless fashion. As UN Secretary-General Kofi Annan noted at the Madrid Summit in March 2005, "international human rights experts, including those of the UN system, are unanimous in finding that many of the measures that States are currently adopting to counter terrorism infringe on human rights and fundamental freedoms."[540]

In the resolution and subsequent action plan, a reference is made to the fact that although there must be full cooperation to counter terrorism and terrorism-supporting activities, there also has to be attention for the protection of fundamental rights in this process, the so called fourth pillar of the action plan.[541] This includes, for example, commitments to respect privacy by restricting the use of intrusion measures of privacy to a minimum.

Although specific descriptions of terrorism are hardly viable in the context of a global platform such as the United Nations, there seems to be developed an intention to cooperate and align measures among the (State) participants to combat the acts of terrorism, keeping in mind human rights whilst doing so.

The recognition of this fact has been remarked by Kofi Anan as cited above and has been stressed on several occasions. In the special international summit on Democracy, Terrorism and security he addressed this issue as follows:

---

[539] *Convinced of the desirability for closer coordination and cooperation among States in combating crimes closely connected with terrorism, including drug trafficking, unlawful arms trade, money laundering and smuggling of nuclear and other potentially deadly materials, and bearing in mind the role that could be played by both the United Nations and regional organizations in this respect;*
And in the same resolution attention for cooperation between nations and institutions
*12. Emphasis is placed on the need to pursue efforts aiming at eliminating definitively all acts of terrorism by the strengthening of international cooperation and progressive development of international law and its codification, as well as by enhancement of coordination between, and increase of the efficiency of, the United Nations and the relevant specialized agencies, organizations and bodies*A/RES/49/60, 17 February 1995, <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N95/768/19/PDF/N9576819.pdf?OpenElement>.
[540] Press Release, Secretary-General, Secretary-General Offers Global Strategy for Fighting Terrorism, U.N. Doc. SG/SM/9757 (10 Mar. 2005), *available at* http://www.un.org/News/Press/docs/2005/sgsm9757.doc.html>.
[541] The four pillars: 1. Measures to address the conditions conducive to the spread of terrorism 2. Measures to prevent and combat terrorism; 3. Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard; 4. Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism.

Human rights law makes ample provision for strong counter-terrorist action, even in the most exceptional circumstances. But compromising human rights cannot serve the struggle against terrorism. On the contrary, it facilitates achievement of the terrorist's objective — by ceding to him the moral high ground, and provoking tension, hatred and mistrust of government among precisely those parts of the population where he is most likely to find recruits. Upholding human rights is not merely compatible with a successful counter-terrorism strategy. It is an essential element in it. I therefore strongly endorse the recent proposal to create a special rapporteur who would report to the Commission on Human Rights on the compatibility of counter-terrorism measures with international human rights laws.[542]

The difficulty is to find a way to apply this policy in international law via resolutions that are accepted and used in the right way by the different Members of the UN.

In its Resolution 2178 (2014), the Security Council reaffirmed the obligation of all States to comply with international human rights law when fighting terrorism, underscoring that, respect for human rights and the rule of law are essential to a successful counter-terrorism effort. It noted that a failure to comply with human rights and other international obligations contributed to increased radicalization and fostered a sense of impunity.

But on the other hand there is a strong urge to fight terrorism and severely punish those who (alledgely) are participating in supporting terrorist activities.

UNSCR 2199 (2015) reaffirmed that "*all States shall ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that such terrorist acts are established as serious criminal offenses in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts, and emphasizes that such support may be provided through trade in oil and refined oil products, modular refineries and related material with ISIL, ANF and all other individuals, groups, undertakings and entities associated with Al-Qaida*."

It is no coincedence that this wording resembles FATF recommendation No. 5, stating that *"countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts.*

With this kind of clauses trust in conditions to protect fundamental rights is not increasing.

6.3.2 Lawfulness of the Legal Instruments of the UN in Anti-Terrorist and AML Regulations

Be it in on another level than the discussions about legal framework of the European Union, there have been discussions about the legislative power of the measures and regulations concerning anti-terrorism and anti-money laundering, issued or supported by the UN, specifically by the Security Council. Sensitive political and economic interests play an overwhelming role in the Security Council of the UN where mainly the permanent Members

[542] Keynote address to the Closing Plenary of the International Summit on Democracy, Terrorism and Security, 8-11 March 2005 in Madrid

define the outcome of the measures that will be accepted in the General Assembly. There is no overwhelming urge to defend the human rights by the permanent Members of the Security Council although reference to these rights is made in almost every resolution or other declaration or legal instrument of the organization and even the Security Council itself. There is an increasing attention being paid to the idea that the Security Council is acting as a global legislator as it considers the fight against terrorism.[543]

The question that arises is: what is the legal effect of the measures by the Council and what are the consequences for the national legal activities on terrorism? Is this not the responsibility of the sovereign state under their own criminal law systems?[544] International regulations tend to be defined in broad and vague terms that can result in competence creep and even abuse when used in prevention and prosecution. This for instance can lead to legitimizing the detention of perceived terrorist whilst bypassing all guarantees of due process and fundamental rights, as in Guantanamo Bay.
This observation can be supported by the remark made by Bianchi for authorities not to be seduced to 'function creep'.[545]The Security Council though, has taken a broad responsibility to counter terrorist actions in a wide sense and is, as stated in Resolution 1373, is "[r]eaffirming the need to combat by all means, in accordance with the Charter of the United Nations, threats to international peace and security caused by terrorist acts, based on the general competence under Chapter VII of the Charter of the United Nations."

It has been defended that the position of the Security Council must be supported by a certain legal power, if not specifically given in the competences in writing then justified by its role by using the doctrines of 'implied powers' and 'subsequent practice.' This reasoning has been invoked to provide legal justification to the evolving practice of the SC, with fervent opponents voicing their concerns about any attempt to reconsider the original role of the SC, namely that of the political peace-enforcer.[546] Referring to Judge Fitzmaurice's dissenting opinion in the ICJ's Advisory Opinion on Namibia "[i]t was to keep the peace and not to change the world order that the Security Council was set up."[547] This should be an 'insurmountable functional limit,' namely peace enforcement, which the SC must not trespass.

Given the high level of the instruments concerned legal measures to be taken by the national authorities are not well described or limited and are instead left to the competence of the 'High contracting Parties.'[548] Although Bianchi states that he regrets that the Security Council gives opportunity to ample extensions of the use of competences by not defining terrorism, I must

[543] Martínez 2008, p. 333.
[544] Bianchi states, for example, that „it is essential that offences created under counter-terrorist legislation, along with any associated powers of investigation or prosecution, be limited to countering terrorism' and not be instrumental to unnecessarily extending the reach of criminal law," 2007, p. 904; Heidelberg 2010, p. 34; Conte 2010.
[545] idem
[546] Bianchi 2007, p. 887, referring to Arangio-Ruiz, 2000, p. 710.
[547] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, Dissenting Opinion of Judge Sir Gerald Fitzmaurice, [1971] ICJ Rep 291, at 294, para. 115.
[548] See for instance the text of Article 9 of the Convention: Upon receiving information that a person who has committed or who is alleged to have committed an offence set forth in Article 2 may be present in its territory, the State Party concerned shall take such measures as may be necessary under its domestic law to investigate the facts contained in the information.

disagree. [549] Terrorism is admittedly not well defined in any legislation but the UN and the SC are putting some effort in this in the Convention.[550]

For others it seems to be clear that when the SC describes 'any act of international terrorism' as *'a threat to international peace and security'* it is acting under the provisions of Article 39 of the UN Charter, and when it decides that all States shall necessarily apply specific measures it does not imply the use of force to fight against that terrorism, it does so under the powers granted by Article 41. Certainly the qualification of an 'emergency' strengthened the position of the SC, concerning the Resolution 1540 (2004) and it was also justified by the urgency of the circumstances.
Martinez is stressing the doubts about the extension of the limits of legality of the actions of the SC: '*Examining the practice of the SC from the beginning of the 1990s, it can be seen that Article 41 has been used with enormous creativity, going far beyond the merely indicative list of examples that the provision contains'* On the other hand he refers to the fact that Article 41 in this case (Res 1540) where it concerned the imminent terrorist threat of Weapons of Mass Destruction the legislative process asked for a speedy and practical solution.[551] Reference is made by Martinez to the press conference prior to the commencement of the debates on this Resolution (2 April 2004), where the President of the SC pointed out that, 'there was a gap in international law pertaining to non-State actors'. So, either new international law should be created, either waiting for customary international law to develop, or by negotiating a treaty or a convention. Both took a long time, and everyone felt that there was an 'imminent threat', which had to be addressed and which could not wait for the usual way.'[552]

The problem is that if these 'legal instruments' as resolutions are to be used and executed by the member states, it is not clear how well-defined and therefore limited the application of the extended power of the SC is.
In a resolution of 2004 the SC lays down a far reaching description of terrorism in a resolution that opens possibilities for wide interpretation. States can use these kind of resolutions to act against groups within and outside their jurisdiction. [553]
Although this also concerns an ample description of acts, it can be considered an acceptable attempt for a definition that is widely used to describe the acts of terrorism and can be interpreted as a definition, although it is an extensive description with still open ends. It may be more beneficial to agree upon a description rather than a definition by reasons of cultural and political differences between states and the fact that states will decide upon these matters on basis of sovereignty.

---

[549] Bianchi 2007, p. 900: *'it would have helped to limit the potential for abuse by reducing the margin of discretion that states have in defining the precise contours of the crimes related to international terrorism in their domestic legal systems'*

[550] See Article 2 b.ofthe International Convention for the surpression of Terrorism, 1999: *Any other act intended to cause death or serious bodily injury to a civilian, or to*
any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

[551] Martínez 2008, p. 334.

[552] Press briefing available at <http://www.un.org/News/briefings/docs/2004/pleugerpc.DOC.htm>.

[553] *Res. 1566 (2004), in which the SC 'recalls that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a State of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature': SC Res. 1566 (2004), at para. 3, see also:*Bianchi 2007, p. 900.

That this wide-ranging description gives opportunity to widespread investigative and surveillance competences of the authorities still stands of course but is another topic. I agree though with the effect that anti-terrorism resolutions and subsequent sanctions can be considered as potential threats to the fundamental human rights of targeted individuals and groups a securely regulated permissible limitation blueprint could add to the acceptance of the limitations as will be the subject of the last chapter. As stated by Bianchi:

Once again, international legal scholarship has stressed the purposes and principles of the Charter, which would limit the SC under Article 24(2), to maintain that 'the inter-action of the principle of good faith with articles 1(1) and 1(3) of the Charter . . . would estop the organs of the United Nations from behaviour that violated . . . the core elements of the human rights norms underpinning Article 1(3).[554]

It must be noted that the United Nations and its organs, including special committees, are bound to their own international legislation such as the Universal Convention on Human rights and the International Covenant on Civil and Political Rights (ICCPR). The application of Article 4 and 17 of the ICCPR would be a way to introduce the permissible limitations to counter terrorism within the acceptable boundaries of human rights. One of the permissible aspects to create regulations to counter terrorism was found in the fight against one of the preliminary sources that makes terrorism possible, the financing of those terroristic actions.

6.4 Anti-Money Laundering and the UN

In a report of the UN the United Nations Office on Drugs and Crime that was published in 2011, broadly in line with the earlier IMF estimates, it was suggested that all criminal proceeds are likely to have amounted to some 3.6% of GDP or around US$ 2.1 trillion in 2009, with an estimated amount available for money laundering equivalent to some 2.7% of global GDP, amounting to some US$ 1.6 trillion. With similar assumptions as above, the amount of money laundered annually in the EU could be estimated at around EUR 330 billion.[555]

Already before the 2001 attacks that initiated resolutions of the Security Council with unprecedented speed as a threat to international peace,[556] there was extensive activity to undermine the preparation of terrorist activities in the UN arena, amongst others on the basis of a resolution of the GA in which a Counter terrorism committee was established in 1996 to investigate the AML activities of possible factions.[557] The actual start of measures against

[555] Estimating Illicit Financial Flows resulting from drug trafficking and other transnational organized crimes, UNODC, October 2011. (no new figures in 2015)

[556] The very next day after the attacks, the Security Council adopted Resolution 1368, in which it regarded those acts, using the very words of Chapter VII of the Charter, as 'a threat to international peace and security', Guillaume 2008.

[557] Recalling further General Assembly resolution 53/108 of 8 December 1998, in which the Assembly decided that the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996 should elaborate a draft international convention for the suppression of terrorist financing to supplement related existing international instruments, ICFST. Gelemerova 2011, p. 49: Two years after the introduction of the US Money Laundering Control Act of 1986, on the eve of global economic liberalization and just before the fall of the Berlin Wall, the international community reached agreement on two documents and these represented the first major steps towards the international cooperation in the fight against money laundering. The two agreements in question were the UN Convention Against Illicit Trafficking in Narcotic Drugs and Psychotropic

money laundering on an international scale stems from national legislative actions within the United States in creating specific AML legislation against drug trafficking. As former US minister Alldridge notes "[h]ad the decision to pursue the war on drugs […] not been taken in the early 1970s, then the concern with the profits of drug dealing and consequently the entire anti-money laundering (AML) industry would not have arisen."[558]

Before the act of money laundering became commonly connected to drug traffic, and later terrorist activities, the term historically stems from illicit activities to hide profits during the prohibition era in the 1920s by the notorious bad guys like Al Capone.[559] The first time the term 'money laundering' was seen in print is during the 'Watergate Affair.'[560]
From that time on, the term money laundering has become common, as well as the activity itself. The need for governmental action against this practice grew. The increasing globalisation of criminal and terrorist activities gave fertile grounds for further development and acceptance of the American initiative for AML legislation.[561] The main legal instruments of the UN to combat money laundering are the 1999 International Convention for the Suppression of the Financing of Terrorism and the resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373. The first international legal use of the term 'terrorist financing' appeared in the UN General Assembly's seminal Declaration on Measures to Eliminate International Terrorism in 1994[562] although the Council specifically referred to 'terrorist financing' for the first time only in Resolution 1269[563] on the financing of Al Qaida concerning drug trafficking and other means to finance terrorism.[564]

Substances ('Vienna Convention'/19 December 1988) and the Basle Statement of Principles on the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering ('Basle Statement'/12 December 1988).

[558] See: reference to Alldridge (2008, p. 438) in Gelemerova 2011, p. 5. For further history and origin of ML. I refer to this theses in which is a.o. referred to**:** Uribe (2003) suggests that money laundering practices date back to at least the Middle Ages when moneylenders invented various mechanisms to cover up their evasion of laws which criminalised usury. Uribe also links the phenomenon of money laundering to the concealment of loot by the pirates of the Mediterranean who deprived Rome of its supplies but were defeated by Pompey in 67 BC. Uribe then describes the pirates who targeted European commercial vessels during the 16th-18th centuries as '*pioneers in the practice of laundering gold*' (Uribe, 2003, p. 131). The comparison may well be appropriate, although there is no clear evidence that pirates' practices of laundering gold ever went beyond the mere concealment of their loot and the bribing of local administrators, p. 29.

[559] See: Gelemerova 2011, p. 31: Saltmarsh 1990; notes that the term 'money laundering' is reputed to have originated from the 1920s, when gangsters like Al Capone and Bugsy Moran opened up laundrettes in Chicago to clean their 'dirty money'. It is possible that during the 1920-30s, the time of Al Capone, police officers coined the term 'money laundering' referring to criminals trying to justify their earnings, 34 Al Capone's brother, Ralph, was indicted on tax evasion charges too. Reportedly a week later after the indictment for tax evasion Al Capone and sixty-eight members of his gang were also charged with some 5000 violations of the Volstead Act (Prohibition), some of them going back to 1922. However, the tax cases took precedence over the Prohibition violations (see Bergreen, 1994). specifically from alcohol trade during the Prohibition era.

[560] As cited by Gelemerova 2011, p.41, oxford dictionary, 2nd edition and:The burglars had reportedly been sent by Nixon and were acting on the orders of CREEP (Committee to Re-elect the President). One of the burglars was James McCord who had a long CIA work record. CREEP was later accused of 'laundering' President Nixon's illegal campaign funds. The Committee was also alleged to have financed its activities via a CIA's front company. See Blum, 1995, and Kangas 1996.

[561]Already starting in 1970, Bank Secrecy Act of 1970 (BSA), or Currency and Foreign Transactions Reporting Act,) PUBLIC LAW 91-507-OCT.26,1970[84STAT

[562] See Murphy 1989. GA Res. 49/60, Annex II, op. paras. 4, 5 (9 December 1994); see also GA Res. 52/165 (15 December 1997); 53/108, ; 54/110 (9 December 1999); 55/158 (12 December 2000).

[563] SC Res. 1269 (19 October 1999).

[564] Bantekas 2003.

The basis of the definition of the financing of terrorist activities and the derived act of money laundering is to be found in this convention and afterwards specified by the OECD, Council of Europe and the European Union.
The reference to financing accounts for any activity that can be defined as 'terrorist activity,' meaning that it is rather extensive. Although the convention seems to be more directed towards the prevention of activities which directly 'fund' terrorist activities. It is interesting that the UN holds any (legal) entity under whose responsibility a terrorist financing (TF) or money laundering operation is taking place as responsible and liable. The UN requires that every participating State to this convention provides legal instruments to follow this requirement.[565]

In this regard, jurisdiction is broadly defined. There is the territorial aspect of the crime pertaining to the nationality of the offender and the location of the crime. The State which is targeted by the crime has jurisdiction when the act is directed against a certain state or government facility (Articles 6 and 7). If a State receives any information, by any means, that such a crime is being committed or is to be committed on its territory or by its nationals (or stateless persons under its jurisdiction), the State is obliged to take investigative measures under Article 9 of the Convention.[566]
Notably parties will not consider these offences as fiscal or political offences so that other jurisdictional or prosecution processes could be applicable and escape from this Convention would be possible.
Although there is a rather implicit reference to the requirements of fundamental rights in the treatment of the suspected offenders, this aspect does not get serious attention.[567] A more explicit article on this subject would be more in line with the spirit of the UN.
In the resolutions of the UN Security council, States are urged to take (any) legal measure or use their authority to counter any terrorist activity or the preparation of financing of terrorist actions. This is clearly stated in, amongst others, in Resolution 1373 which "[d]eclares that acts, methods, and practices of terrorism are contrary to the purposes and principles of the United Nations and that knowingly financing, planning and inciting terrorist acts are also contrary to the purposes and principles of the United Nations." This resolution specifically refers to the international standards of human rights[568]

These resolutions and measures can be deemed lawful given that they originate from the International Convention for the suppression of the Financing of Terrorism[569] and several

[565] Article 5.1; Each State Party, in accordance with its domestic legal principles, shall take the necessary measures to enable a legal entity located in its territory or organized under its laws to be held liable when a person responsible for the management or control of that legal entity has, in that capacity, committed an offence set forth in Article 2. Such liability may be criminal, civil or administrative.
[566] Article 9; Upon receiving information that a person who has committed or who is alleged to have committed an offence set forth in Article 2 may be present in its territory, the State Party concerned shall take such measures as may be necessary under its domestic law to investigate the facts contained in the information.
[567] Article 17; Any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to this Convention shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law.
[568] States must also fulfill their obligations under the Charter of the United Nations and other provisions of international law with respect to combating international terrorism and are urged to take effective and resolute measures in accordance with the relevant provisions of international law and international standards of human rights for the speedy and final elimination of international terrorism, A/RES/49/60,17 February 1995, p. 5, <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N95/768/19/PDF/N9576819.pdf?OpenElement
[569] This convention requires parties to take steps to prevent and counteract the financing of terrorists, whether direct or indirect, through groups claiming to have charitable, social or cultural goals or which also engage in illicit activities such as drug trafficking or gun running; Commits States to hold those who finance terrorism

resolutions of the General Assembly of the United Nations against (the financing of) terrorism.[570] It remains, however, questionable whether a far-stretching legislative measure from the Security Council is acceptable from a legislative perspective.

6.4.1 Interaction between UN and Financial Action Task Force (FATF)[571]

Maybe because it was deemed politically acceptable to start a more business-orientated set of recommendations or perhaps there was a substantial business interest by industry, the fact is that anti-money laundering started to be a serious issue to regulate on the OECD platform as an economic problem. As Kofi Anan stressed in his address to the 2005 summit in Madrid, the activities of the OECD in this context could be followed by the UN to counter the terrorist supporting activities. He said "[w]e also need effective action against money-laundering. Here the United Nations could adopt and promote the eight Special Recommendations on Terrorist Financing produced by the OECD's Financial Action Task Force [FATF]."[572]

On their turn the FATF refers to the UN in this respect stating that:

Each country should take immediate steps to ratify and to implement fully the 1999United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

The 2003 UNODC Model is updated by the 2009 and the 2012 updated model provisions. The updates are based upon the relevant international instruments concerning money laundering and the financing of terrorism, the FATF 40+9 Recommendations and best practices. Although

---

criminally, civilly or administratively liable for such acts; and Provides for the identification, freezing and seizure of funds allocated for terrorist activities, as well as for the sharing of the forfeited funds with other States on a case-by-case basis. Bank secrecy is no longer adequate justification for refusing to cooperate.

[570] General Assembly resolution 51/210 of 17 December 1996, paragraph 3, subparagraph (f), in which the Assembly called upon all States to take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities, and in particular to consider, where appropriate, adopting regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes without impeding in any way the freedom of legitimate capital movements and to intensify the exchange of information concerning international movements of such funds. Recalling also General Assembly resolution 52/165 of 15 December 1997, in which the Assembly called upon States to consider, in particular, the implementation of the measures set out in paragraphs 3 (a) to (f) of its resolution 51/210 of 17 December 1996, Recalling further General Assembly resolution 53/108 of 8 December 1998, in which the Assembly decided that the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996 should elaborate a draft international convention for the suppression of terrorist financing to supplement related existing international instruments, UN treaty series, *Vol. 2178, 1-38349,* <*http://treaties.un.org/doc/publication/UNTS/Volume%202178/v2178.pdf)*>.

[571] The FATF is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions, started with eleven members, and now has 38 Members, 8 associate members and 25 observers, with amongst them, Interpol and Europol.

[572] Until now I did not find document from which it is made clear that the birth of the FATF was within the context of OECD. Still the seat of FATF is on the same address as the OECD.

not an official member, the FATF participates (often) in the United Nations Counter-Terrorism Committee (UN CTC).[573] The model provisions are intended to be a resource in drafting legislation to address money laundering and the financing of terrorism. Combined, the provisions incorporate a legislative base for many of the requirements of the relevant international instruments and the FATF 40+9 Recommendations. The provisions also strengthen or supplement these standards in some respects. They suggest an approach both to criminally confiscate and civil forfeit proceeds, instrumentalities and terrorist property.

The roles of the UN and FATF are quite different. The FATF is in essence a non-formal inter-governmental organization based in Paris, within the walls of the OECD, which develops policy rules to counter the financing of terrorist activities. It does not create legally binding regulations or rules but has created a set of recommendations that is followed by most financial authorities. The interaction though between UN CTC and FATF is quite strong. In the words of the FATF Executive Secretary Rick McDonell this role is explained as follows:

First of all, although the roles are obviously different between the FATF and the UN, from the FATF's point of view the UN plays the primary role in the fight against terrorist financing by establishing a framework of binding international legal obligations. For example, as has been stated already this morning, the International Convention for the Suppression of the Financing of Terrorism (1999), and the Terrorist Financing Convention of Security Council Resolution 1373 in particular. In relation to those instruments, the FATF complements and reinforces the work of the United Nations through adopting a comprehensive set of measures (called the FATF Recommendations) that help countries to combat terrorist financing and therefore, hopefully, effectively implement the UN Recommendations in this area.[574]

Most State authorities are very serious in adapting the FATF set of principles and recommendations and are inclined to include this set within their constitutional and financial systems. Additionally, the provisions provide additional measures that a State may consider suited to effectively combat money laundering and the financing of terrorism in the national context. The strong national policy context is, for instance, clear in the meeting of the ministers of finance and national bank directors of the G20 in November 2012 where they committed full adherence to the FATF objectives and recommendations that will be elaborated in the next paragraph.[575] Although EU directives formally have a stronger legal power, in essence the power of the recommendations is not to be underestimated because most of the UN, EU and national AML legal measures are based upon the FATF documents.

6.4.2 The FATF Recommendations

[573] For instance at the meeting which was held on 20 November 2012 with Member States and relevant international and regional organisations. The event was aimed at raising awareness of the threat of terrorist financing, and focused on the measures required to prevent and suppress such activity.

[574] *Remarks by the FATF Executive Secretary Rick McDonell on 'Tackling terrorism financing: the revised FATF standards' at the Special meeting of the United Nations Counter-Terrorism Committee with Member States and relevant international and regional organizations on preventing and suppressing terrorist financing 20 November 2012[http://www.fatf-gafi.org/fr/themes/gafiengeneral/documents/tacklingterrorismfinancingtherevisedfatfstandards.html*

[575] *'We remain committed and encourage the FATF to continue to pursue all its objectives, and notably to continue to identify and monitor high-risk jurisdictions with strategic Anti-Money Laundering/Counter-Terrorist Financing (AML/CFT) deficiencies*'. G 20 meeting Communiqué of Ministers of Finance and Central Bank Governors of the G20 Mexico City, 4-5 November 2012.

To provide some background in addition to the former section, I will explain the development of FATF and the FATF set of recommendations. [576] In response to a mounting concern over money laundering, FATF was established by the G-7 Summit that was held in Paris in 1989. To coordinate the action and influence a harmonized policy under the guidance of the United States, the G-7 Heads of State or Government and President of the European Commission convened in this Task Force from the G-7 member States, under the flag of the OECD. As formally decided by those members, the Task Force was given the responsibility for examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering. The reason for this initiative, according to FATF, was that those transactions posed a threat to the banking system and to financial institutions. The common understanding that these illicit transactions became a 'universal threat' to the global financial system had been discussed at a global (UN) level, the year before in 1988, at the 'Vienna Convention.'[577] In April 1990, less than one year after its creation, the FATF issued a report containing a set of *Forty Recommendations*, which were intended to provide a comprehensive plan of action needed to fight money laundering. This initiative was heavily supported by the United States, which wanted to have control over the illegal transactions that supported drugs transactions.

This forum of international cooperation was a perfect place for the United States to enhance their policy and harmonization of the battle against illicit financial support of drug trafficking and later- terrorist activities, covered by a set of 9 special recommendations.[578] These 'extra' special recommendations were, not surprisingly, initially added by the United States initiative after 2001. In 2001, the development of standards in the fight against terrorist financing was added to the mission of the FATF. In October 2001 the FATF issued the 'Eight Special Recommendations' to deal with terrorist financing. The continued evolution, as well as the attention of governmental authorities for this issue of money laundering techniques related to terrorism, led the FATF to revise its standards comprehensively in June 2003. In October 2004 the FATF published a 'Ninth Special Recommendation', further strengthening the agreed upon international standards for combating money laundering and terrorist financing.

The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.
FATF had quite some leverage to enforce adaption to its rules by publishing blacklists of countries that did not enforce its recommendations.[579]

---

[576] FATF Recommendations, *IX Special Recommendations*, <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html>.
[577] UN Convention Against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances: Vienna Convention, 19 December 1988.
[578] As the Vienna Convention alone was not sufficient to establish a global anti-money laundering regime, the FATF stepped in to speed up the process. The USA needed an international forum to promote or, if necessary, to impose policies worldwide and the FATF became this forum. It was created to help enhance international cooperation and assess the results of anti-money laundering policies globally. Gelemerova, p. 51.
[579] See Gelemerova 2011, p. 52: In 1998, when it was recognised that many countries still lacked an adequate anti-money laundering regime, the FATF launched the Non-Cooperative Countries and Territories (NCCT) Initiative. Unless evaluated countries (and territories) complied with FATF's standards they risked to be branded and blacklisted as 'non-cooperative', and consequently to be rejected as partners in the international payment system with serious potential consequences for their economy (see Stessens, 2000). The list stopped to be updated since 2007 without giving reasons.

The FATF nowadays can be considered as the global standard-setting organization for measures to combat money laundering, terrorist financing, and (most recently) the financing of proliferation of weapons of mass destruction. Although it is an intergovernmental body with just 38 members, directly or indirectly it effectively covers almost 200 180countries through a global network of FATF-style regional bodies and Financial Intelligence Units (FIU's) that form the fundamental structure of FATF and the application of the recommendations. [580] In addition, the Council of Europe is connected to FATF via a Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)[581]. The European Union has followed these initiatives by issuing Anti Money Laundering directives.

6.4.3 The Essence in Controlling Money Laundering: The FIU Construction[582]

Financial Intelligence Units (FIUs) are governmental or semi-governmental organizations that are designed to receive referrals of unusual or suspicious financial transactions as perceived so by financial and other institutions. The role of a FIU is to process and analyse the unusual transaction reports from the reporting entity and submit its report to the Legal Enforcement Agency if the transaction is considered to be suspicious enough to warrant further criminal investigation.

According to the considerations in the Third European AML directive, the role of the FIU can vary in intensity, be it by taking an administrative role or already participating in the investigative process. One of the essential activities of the FIU will be the possibility to exchange data with other FIU's:

(29) Suspicious transactions should be reported to the financial intelligence unit (FIU), which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIUs, allowing them to conduct their business properly, including international cooperation with other FIUs. [583]

The FIUs do not have the same powers and legal position in all European (and other) countries. This can cause problems in the actual cooperation and exchange as required in the directive. FIUs are intended to include powers to use compulsory measures for the production of records held by financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs) and other natural or legal persons, for the search of persons and premises, for taking witness statements and for the seizure and obtaining of evidence. Further it is stressed that countries should ensure that competent authorities conducting investigations are able to use a wide range

[580] 199 in 2015, source: OECD/FATF.

[581] MONEYVAL was established in September 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessment exercises of the anti-money laundering measures in place in Council of Europe member states, which are not members of the Financial Action Task Force * (FATF). The effort includes encouraging jurisdictions to improve their anti-money laundering measures in keeping with the FATF Forty + 9 Recommendations [http://www.fatf-gafi.org/pages/moneyval.html]

[582] This paragraph will be partly produced in delivery D.2.3 of the European FP 7 project, HEMOLIA, final report May 2014.

[583] 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, consideration 29.

of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing.
These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery.[584]

The reason why investigations are started, purpose specification, or any recommendation how to translate the requirements of the directive and FATF are left for the countries to decide. The balancing of these far-reaching requirements with considerations of privacy is not considered an issue. There remains a gap in considering how privacy fits within the far-reaching recommendations and requirements

6.4.4 Terrorist Financing in FATF: the Recommendations [585]

The 40 Recommendations provide a complete set of counter-measures against money laundering (ML) covering the criminal justice system and law enforcement, the financial system, its regulation and international co-operation.

As pointed out earlier, the influence on UN and EU legal AML framework and consequently national law is substantial, therefore this section provides a short overview of the key recommendations. Special attention is given to those recommendations that could enlarge the risk of misuse, competence creeping and which could endanger the use of personal data.

The first recommendation concerns the scope of the measures. Countries should include the crime of money laundering with all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach).

The second recommendation concerns national cooperation and coordination. The third recommendation requires consistency with the principles of the Vienna and Palermo Conventions in extension of applicability of criminal liability, and, where that is not possible, civil or administrative liability to (non-natural) legal persons. The fourth recommendation concerns measures for the identifying, tracing and confiscation of laundered property. Recommendations 5-9 are directed at terrorist financing and financing of proliferation.

In the fifth recommendation many regulatory doors are opened by the requirement that countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists, even in the absence of a link to a specific terrorist act or acts. The sixth recommendation states that countries should ensure that such

---

[584] Further, the following requirements are added:
In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts.They should also have mechanisms to ensure that competent authorities have a process to identify assets without
prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

[585] International standards on combating money laundering and the financing of terrorism & proliferation the FATF recommendations February 2012, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>.

offences are designated as money laundering predicate offences and targeted financial sanctions regimes to comply with United Nations instruments.[586]

Recommendations 10 and 11 concern customer due diligence (CDD) and record-keeping; the 11th requires financial institutions to keep records of all financial transaction for five years for the authorities. From a personal data protection perspective, it is interesting to note the description of the files and documents because it is rather wide-reaching:

copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Recommendations 12-16 relate to additional measures for specific customers and activities, such as licensing money transfers, wire transfers and pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. Risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks. Recommendation 12 specifically addresses politically-exposed persons.

Recommendations 17-19 concern reliance and control mechanisms. Recommendations 20 and 21 are about the reporting of suspicious transaction to the FIU and the protection of involved persons. Recommendations 22 and 23 describe measures to be taken by financial institutions and non-financial businesses and professions to prevent money laundering and terrorist financing, describing the due diligence requirements and addressing the parties involved such as notaries, lawyers, financial institutions, trust companies, and casinos, among others. Recommendations 24 and 25 concern transparency and beneficial ownership of legal persons and legal arrangements to prevent misuse. Recommendations 26- 28 describe powers and responsibilities of competent authorities and other institutional measures, regulations and supervision. The authorities must have the powers to initiate regulation and also have supervision to ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing.

It is not specified which authority (supervisor) will be vested with these powers. It would likely be a national bank or a ministry of finance, as was seen in the European 'freeze directive' pertaining to the Russian-Ukrainian conflict.[587]

Recommendation 28 is concerning documents, directed toward the DNFBPs as mentioned under 22 and 23. Recommendations 29, 30 and 31 require the operational Financial Intelligence Units and law enforcement agencies to use all possible means to fight money laundering and Financing Terrorist Activities (FTA).

[586] The United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).
[587] 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 EU, 29-4-2014, L 127/39.

Recommendations 32-34 are about administration, statistics and cash transport. It becomes more relevant again arriving at recommendation 35 where a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative is required for those legal and natural persons, including financial institutions and DNFBPs that do not comply with the contents of the document. Recommendations 36 to 40 are all about international cooperation, mutual assistance and obligations not to withhold any information or hamper the exchange of this information. The last recommendation requires the assured extradition of persons that will commit AML and FTA crimes.

Additionally, recommendations 17-21 describe other measures to deter money laundering and terrorist financing, including the installation of a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

6.4.4.1 The FATF review of 2012

In February 2012, the FATF completed a thorough review of its standards (recommendations) and, after a three year review process, published the revised FATF Recommendations.[588] This revision is, according to the FATF, intended to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. The standards have been expanded to deal with new threats such as the financing of proliferation of weapons of mass destruction, but also to be clearer on transparency and tougher on corruption. This has resulted, according to the FATF, in a stronger and clearer set of standards. The question is whether this observation is correct. What is clear is that there is an extension of the application of the rules to (criminal) acts that may be supported by money laundering. The reference to UN instruments is accentuated to give a more global and human rights stamp to the measures. According to the FATF the main changes are the following of UN SC instructions in case of targeted financial sanctions against financing weapons of mass destruction:

- lifting of corporate veils and stooges behind terrorist financing;
- the introduction of better advanced techniques for FIU's and Law enforcement and
- better international cooperation between them.

Regarding the review of the recommendations, there is some resistance to the actions of FATF to extend the application of the recommendations, for example to tax crimes.[589]

Also included is the new recommendation of customer due diligence measures wherein there is a "possibility of exemptions from identifying the beneficial owner, unless there are identified money laundering and terrorist financing risks."

It is not very clear when this exception is possible, under what circumstances and how this is guaranteed in the law. The same accounts for the measures taken in the sphere of the specific

[588] The review document is updated and adapted continuisly. http://www.fatf-gafi.org.

[589] The concerns relate in particular to: (i) the scope of tax crimes, with a strong preference indicated that only serious tax crimes should be included; (ii) the lack in expertise and the inherent difficulty for the private sector. in detecting tax crimes; and (iii) the need for a level playing field, FATF response to the public consultation on the revision of the FATF recommendations, p. 3.

circumstances of the life insurance industry when dealing with beneficiaries of life insurance policies.

Another problem that remains concerns the so-called 'risk based approach' that is considered essential in the revision, which is not very well explained and is kept rather vague.[590]

Of course there is always the possibility to lean on more extreme investigation when there is a heavier risk, whenever and however these risks are defined. Of course this should be decided on the basis of balanced considerations and objective legal standards. With regards to those who may be politically-exposed, the new recommendation twelve concerns primarily corruption and blackmail rather than ML and terrorism although they can be considered targets from both perspectives.

Considering the view of respondents to the review by FATF it is interesting to see the comments concerning privacy and data protection that are considered obstructive to the purposes of AML.

"The FATF considered the concerns raised by the private sector that data protection and privacy laws in some countries could limit intra-group cooperation and reliance, and that financial institutions and DNFBPs should not be obliged by the rules of one regulator to breach the rules of another."

This issue is not regarded from the perspective of caring for the position of the 'innocent' individuals and to protect their fundamental rights, but from the perspective of obstruction of exchange of information. Because of the sensitive character of the issue, a very vague text leaves the matter for further elaboration, without taking any steps to support the protection of privacy or even to recognise the importance of protecting fundamental rights.[591]

Considering the international cooperation, one could say that there is a hint to legal guarantees for legal certainty and protection of personal information, although the recommendations (36-40) are more directed towards confidentiality and security of the exchange of relevant information between the FATF players. Further, logically, it is considered to be of the utmost importance to harmonize the typologies and concepts and terminology as well as understandable and useful feedback as a new recommendation (29).

This seems to be a logical 'conditio sine qua non' but in practice this is still an objective that is not fulfilled and forms a great source of legal uncertainty. This is not solely a problem from the FATF perspective as was also made clear in the evaluation of the third AML directive of the European Union. This will be explained in the next section.

6.4.5 Describing Financing of Terrorism and Money Laundering in European

[590] *under the risk-based approach, the scope and depth of those measures may vary, and it may even be possible for there to be exemptions from the requirement to identify and verify the beneficial owner in strictly limited and defined circumstances, when there is proven low risk of money laundering or terrorist financing*.

[591] This is a complex area in which the FATF is not able to act unilaterally, and the FATF recognises that it will have to work closely with other relevant international bodies. The FATF is considering a coordinated process to further examine the issue. Nonetheless, in order to facilitate the effective implementation by the private sector on the FATF Recommendations, the revised Standards also seek to promote cooperation between relevant authorities both domestically and internationally. Supervisors should also work with their counterparts to facilitate intra-group cooperation and exchange of information by the private sector. See EU review, p. 9.

Perspective

The EU adopted the aforementioned regulations concerning the crimes of money laundering (ML) and financing of terrorist activities in the so called AML directives.[592] The directive is transposed in national law of the Member States. Therefore it ought to be ultimately clear what the definition of those criminal activities is. In the case of money laundering we see that the definition of money laundering has been stretched to the handling of any good or service of financial value with a (potentially) illegitimate purpose of the "achievement of a misleading appearance of 'cleanness', or legitimacy 'as having an apparently legal source."[593]

In a wider sense, the European AML directives describe money laundering and Terrorist Financing as consisting of a long list of possible money laundering activities, as transferring funds in all possible ways to disguising illicit origin of property and the use of these activities for or assisting terrorist activities.[594]

Clearly the European AML directive considers a wide circle of activities as fitting under the description of money laundering. It is not clear whether participation in the money laundering activities has to be done 'knowingly' in order to be considered criminal. However, factual circumstances seem to be enough indication of the 'criminal' intentions of the persons and institutions concerned. [595]

The current EU framework in Article 3(5) (f) of the Third AMLD and Article 3 (4) f of the Fourth AMLD take an 'all serious crimes' approach as in the (illegal) retention directive, and includes within its scope all other criminal offences which carry a punishment of imprisonment based on a mixture of maximum and minimum thresholds, differing in the Member States, in The Netherlands with a maximum of four years imprisonment.

---

[592] During the writing of this thesis, the so called Third AML directive was replaced by the Fourth AML directive: 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, EJEU L 141/73, 5 June 2015.

[593] Gelemerova 2011, pp. 62 and 65.

[594] *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 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 counseling the commission of any of the actions mentioned in the foregoing points.

[594] *For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should 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 of 13 June 2002 on combating terrorism.*

[595] Article 1.5, Third AML Directive.

Therefore the possibilities to limit the applications of fundamental freedoms, such as privacy, will be possible in a broad sense. Nevertheless, there is homage paid to the ECHR in recital 48 of the directive.[596] The Fourth AMLD refers to privacy and innocence as stated within the European fundamental rights framework[597] Of course that does not mean that circumstances under which these rights are limited will not be taken into account. The other uncertainty is that no clear difference is made between the act of money laundering and the act of terrorist financing in the directive. Therefore, also on a national level, no differentiation is made between those two acts, nor in material criminal law in defining the act, nor in the procedural criminal law.

To put it in clear perspective, the crime of ML and TF is broadly defined, which leaves uncertainty as to its application. In addition, the possible application of the limitation principles of international law is extended, which adds to the uncertainty. Finally, this means that the exceptions to privacy are broadened because in the new rules in FATF 2012 and the Fourth AMLD which are based on risk-management there is:

a. an extension of the description of ML and TF
b. an extension of the application of the limitation principle in international and national law.

This aspect is also recognized, but not at all criticized in the Third European AML directive:

Although initially limited to drugs offences, there has been a trend in recent years towards a much wider definition of money laundering based on a broader range of predicate offences. A wider range of predicate offences facilitates the reporting of suspicious transactions and international cooperation in this area.[598]

It is quite logical that the reporting of suspicious transactions will increase in this way but does that also increase the actual image of ML and TF acts? The same 'problem' of uncertainty is recognized by the United States:

United States anti-money laundering efforts are impeded by outmoded and inadequate statutory provisions that make investigations, prosecutions, and forfeitures more difficult, particularly in cases in which money laundering involves foreign persons, foreign banks, or foreign countries.[599]

A proposed solution to solve the 'problem' could be by extending the provisions. Although understandable in the view of the crime fighters, the principle of 'lex certa', comes under pressure. Because of a broadening of the 'definition of crimes', the observation of suspicious areas and subjects as such in the international and national description of crimes the overly

[596] This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the European Convention on Human Rights.
[597] (65) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.
[598] Recital 7, Third AML Directive. Referred to in recital 3 of the Fourth AML Directive
[599] 'International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001', part of the 'Patriot Act', 115 STAT. 296 Public Law 107–56— 26 October 2001.

inclusive understanding of money-laundering crimes is risky because it potentially targets innocent bystanders.[600]

This is certainly the case if there is an extension of ML to 'potential' transactions, as proposed in The Netherlands.[601] As stated by Marianne Hirsch Balin in her 2012 dissertation,

Contiguous to the objectives of criminal procedural law, (…) the Dutch CCP as established in 1926 clearly formulates that the main goal of criminal procedural law is to establish the truth in order to convict the guilty and to prevent the conviction of those who are innocent.[602]

This means that the legal certainty of what is considered a crime should not change 'on the way', nor should it be defined or described in such an open wording that the danger of 'offence-creep' is finding its way into the legal system, even if there is a need for adaption to the circumstances. The Dutch legal system also follows the wide interpretation of using or having 'any object of value' or giving any help or support to commit a crime as defined in Article 83 of the Dutch CC as being a terrorist crime. It involves a series of crimes, 'as long as they are committed with a terrorist intention.'[603] Terrorist intention is explained in the following Article 83(a) as to

'have the objective to bring fear to the population or part thereof, or force a governmental or other international organization to act or abstain from the act, or disrupt or destroy the constitutional, social, or economical structure of a State or international organization.'[604]

Also concerning the access of agencies and institutions to sensitive financial information under circumstances a wider range of acces can be provided for, going beyond the limits of the Fourth Directive.[605]

---

[600] As the tightening of controls in the financial sector has prompted money launderers and terrorist financers to seek alternative methods for concealing the origin of the proceeds of crime and as such channels can be used for terrorist financing, the anti-money laundering and antiterrorist financing obligations should cover life insurance intermediaries and trust and company service providers. Recital 15, Third AML Directive.

[601] To ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities, and that jurisdictional disputes do not hinder examination of compliance by financial institutions with relevant reporting requirements, 115 STAT. 298.

[602] Hirsch Ballin 2012, p. 39.

[603] Dutch Act for the prevention of ML and TF (Wet ter voorkoming van witwassen en financieren van terrorisme) Article 1.under i. *financieren van terrorisme:*
1°. opzettelijk verwerven of voorhanden hebben van voorwerpen met geldswaarde, bestemd tot het begaan van een misdrijf als bedoeld in artikel 83 van het Wetboek van Strafrecht;
2°. opzettelijk verschaffen van middelen met geldswaarde tot het plegen van een misdrijf als bedoeld in artikel 83 van het Wetboek van Strafrecht; of
3°. het verlenen van geldelijke steun, alsmede het opzettelijk werven van geld ten behoeve van een organisatie die tot oogmerk heeft het plegen van misdrijven als bedoeld in artikel 83 van het Wetboek van Strafrecht;

[604] Translation of: *Onder terroristisch oogmerk wordt verstaan het oogmerk om de bevolking of een deel der bevolking van een land ernstige vrees aan te jagen, dan wel een overheid of internationale organisatie wederrechtelijk te dwingen iets te doen, niet te doen of te dulden, dan wel de fundamentele politieke, constitutionele, economische of sociale structuren van een land of een internationale organisatie ernstig te ontwrichten of te vernietigen.*

[605] (14) (…) Member States should also ensure that other persons who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax crimes and fraud, are granted access to beneficial ownership information, in accordance with data protection rules. The persons who are able to demonstrate a legitimate interest should have access to information on the nature and extent of the beneficial interest held consisting of its approximate weight. (15) For that purpose,

In conclusion, the definition of both 'terrorism and money laundering' are kept intentionally rather vague and provide an open description of offence so that the contents can be adapted to the circumstances. Also the access to information by undescribed agencies is provided for without much guarantees. This is a dangerous development in criminal law. The reason for that is that this 'crime' is developed under political pressure of the United States, incorporated by the United Nations and the FATF. These observations will be elaborated in the next sections.

6.4.6 Unpacking the Ambiguity in the Definitions: Terrorism[606]

As described above, it was not possible to agree upon a global definition of terrorism. For the first time, a really extensive description of terrorism is given in the EU Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism and the council framework decision of 13 June 2002.[607] Although this description is too broad to be considered as a definition, it is nevertheless extensive in the acts it enumerates.[608]

This is a very broad and seemingly enumerative description of terrorist action, or, more precisely, actions with terrorist intent. Most of the acts described in the framework decision are already criminalized in national and criminal codes and relevant treaties. However, importantly, it is the intention of the commission of these acts that may qualify them as terrorism. In the Council Framework Decision 2008/919/JHA this list is extended by several supporting activities, including provocation, recruitment and training. There is a danger to a too wide-reaching in its description of terrorist acts that are already criminalized.

Although at the UN level there is still no commonly agreed definition of terrorism and acts of terrorism, the UN General Assembly Resolution 49/60 entitled 'Measures to Eliminate

---

Member States should be able, under national law, to allow for access that is wider than the access provided for under this Directive.

[606] For a general overview of all AML legislative and policy actions of the EU: <http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm#overview>

[607] EU Council Framework Decision of 13 June 2002, EJ, L 190/1 and on combating Terrorism Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)/(2002/475/JHA).

[608] *On combating terrorism, Article 1: Act that their nature or context, may seriously damage a country or an international organisation where committed with the aim of: — seriously intimidating a population, or — unduly compelling a Government or international organization 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, shall be deemed to be terrorist offences:(a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person;(c) kidnapping or hostage taking; (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;(e) seizure of aircraft, ships or other means of public or goods transport; (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life; (i) threatening to commit any of the acts listed in (a) to (h).* See the description of the process of defining terrorism in Chapter 6.

International Terrorism,' contains a provision describing terrorism. Interesting is the aspect that neither reason whatever can justify these acts:

Criminal acts intended or calculated to provoke a State of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them'. [609]

National laws use mere descriptions, not definitions, in their criminal law. Limiting measures are given in separate laws as stated in the 2002 European Union framework decision based upon these general descriptions of *'offences under national law, which, given their nature or context, may seriously damage a country or an international organisation'.*

This general description can also be found in the 2010 report of Europol:

The TE-SAT 2010 mentions criminal acts with the potential to seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country [as an act of terrorism].[610]

It is not clear though if these acts always considered to endanger national security. One may presume that this will be a consideration in taking far-reaching measures to limit the privacy of natural persons by searches and seizures of the personal information of persons considered 'persons of interests' connected to the determination of threats.

In 2015 the European Commission proposed a directive on combatting terrorism, to replace the framework decision on terrorism. [611] In this proposal, that formed a reaction on ISIS threats and terroristic attacks on European soil in the beginning and the end of that year in Paris, there is a rather open ended system in its provisions going beyond the specifcs of even a directive.

As stated in explanatory memorandum there is a tendency to increase the competences of the Member states in open ended policy and even legislation to counter evolving terrorism,
To

" facilitate investigation and prosecution of all relevant terrorist modus operandi, avoiding significant loopholes in the criminal justice response.

In this spirit, the draft Directive also proposes to criminalise the following behaviours: attempt of recruitment and training, travel abroad with the purpose of participating in the activities of a terrorist group, and the financing of the various terrorist offences defined in the draft Directive'.[612]

Concerning the exchange of information between competent law enhancement authorities concerning reference is made to existing EU legislation to create national contact points and

[609] GA resolution 49/60, 9 December 1994.
[610] TE-SAT 2010. Report, p. 6, <http://www.consilium.europa.eu/uedocs/cmsUpload/TE-SAT%202010.pdf>.
[611] **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, 2.12.2015 COM(2015) 625 final 2015/0281.

[612] Idem, p. 8.

exchange spontaneously information where there are reasons to believe that the information could assist in the detection, prevention or investigation of terrorist offences.[613]

6.4.7 Financing Terrorism

In addition to terrorism, as also confirmed in the proposal of the former paragraph, it is clear that the financing of terrorism is considered a legitimate reason to limit the contents of privacy rights. Within the European Union the actual legislation against money laundering has been mainly embodied in the fourth[614] and third Anti-Money Laundering Directive,[615] preceded by two other directives and other European regulations. In this section I will concentrate on the Third Anti-Money Laundering Directive ('third AML') as it was evaluated before the fourth AML Directive was accepted. For reasons of completeness I refer to the fourth AML Directive and the other legislative measures that have been taken in the existing AML and TF framework of the EU, notably another directive, two regulations and an EU Council decision.[616] The Fourth AML Directive is mainly changed on basis of the 2012 FATF recommendations.

As stated in the 2nd recital of the Third AML Directive, the reason for this legislation is:

That 'massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.

In the assessment report of revision of the Third AML Directive this positive outcome is severely called into question given that it is estimated that only 0,2% of the dirty money streams are discovered.[617]

---

[613] Council Framework Decision 2006/960/JHA,11 Decision 2008/615/JHA (Prüm-Decision),12 particularly in combating terrorism and cross-border crime and the Decision 2005/671/JHA. And the protocol, no,7.

[614] The proposal was accepted in May 2015.
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 EU L141/73.

[615] 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, OJ EU, L309/15, 25 November 2005.

[616] Directive 2006/70 containing a number of implementing measures with respect to Politically Exposed Persons, simplified customer due diligence procedures and limited exemptions. Regulation 1781/2006, which ensures traceability of transfers of funds by requiring information on the payer to accompany transfers of funds for the purposes of the prevention, investigation and detection of money laundering and terrorist financing. Regulation 1889/2005 on controls of cash, which requires persons entering or leaving the EU to declare cash sums they are carrying if the value amounts to EUR10 000 or more; EU Council Decision 2000/642 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. A number of EU legal instruments imposing sanctions and restrictive measures on governments of third countries, or non-state entities and individuals.

[617] According to the October 2011 United Nations Office on Drugs and Crime (UNODC) study, the amount of funds intercepted by law enforcement is estimated to amount to less than 1% of the total funds laundered, and actual seizures amounted to less than 0.2%. See: Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial systems for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying

This Third and Fourth Directive was preceded by the earlier policy concerning AML and the 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.[618] Because there was a general concern amongst Member States that money laundering could disintegrate the financial system of the internal market, the conclusion was that a general coordination of this field was imperative to decrease the risk of damaging the financial system and the free flow of financial data and services between Member States

The regulatory framework, and more specifically the AML directives, were intended to result in measures by Member States to prohibit money laundering and to oblige the financial sector, comprising of credit institutions and a wide range of other financial institutions, to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities.

Until now, the reference to protecting individuals and specifically personal data was not the most eye catching aspect of the legislative actions. The recitals of the third AML Directive refer also to other organizations that have taken actions against money laundering, more in particular to the Recommendations of the Financial Action Task Force (FATF), which is also by the European Union considered the foremost international body active in the fight against money laundering and terrorist financing. It is recognized that within the Directive the FATF series of the revised 40 recommendations will be implemented in the new legislative product that are issued in a fourth directive, or at least an adapted third directive.[619] The FATF also clearly was the source of the adaptive initiatives for the directive as was stated in the statement on the review/evaluation of the directive:

Broad support was expressed for the proposed alignment to the revised Financial Action Task Force (FATF) standards and for greater clarification of certain issues, in particular in the area of data protection and cross-border situations.[620]

Most of the reactions were from business-and public sector and are clear not instigated from a privacy or data protection perspective. [621] The evaluation is quite analogous to the review of the FATF as described in the previous section. In the proposal for a new text, further mentioned as the Fourth AML Directive, we clearly find the influence of FATF, although the introductionary text of the proposal of the Fourth AML suggests that the (revised) text of the directive is complementary to the FATF recommendations:

---

transfers of funds, 08 February 2013 6230/13 ADD 1, 2013/0024 (COD) 2013/0025 (COD). Point 28, Available at: <http://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vj725dcy4fzm>.

[618] OJ L 166, 28 June 1991, p. 77. Directive as amended by Directive 2001/97/EC of the European Parliament and of the Council (OJ L 344, 28 December 2001, p. 76).

[619] Initially planned to be Autumn 2012, in concept published in February 2013, Agreed common position (Council EU) June 13th 2014Interinstitutional File: 2013/0025 (COD) [http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010970%202014%20INIT]

[620] Report from the Commission to the European Parliament and the Council on the application of Directive 2005/60/EC, July 2012, <http://ec.europa.eu/internal_market/company/docs/financial-crime/072012_feedback_statement_en.pdf>.

[621] Consisting of 77 contributions. Contributions were made by public authorities, civil society, business federations and companies in several fields (including financial services, gambling sector, legal professions, real estate sector, trust and company service providers), allowing for a broad representation of various stakeholders. Replies originated in 15 EU Member States and in some countries from outside the EU (e.g. Jersey). 21 of the 77 replies, i.e. 27%, were provided by pan-European organizations.

A revision of the Directive at this time is complementary to the revised FATF Recommendations, which in themselves represent a substantial strengthening of the anti-money laundering and combating terrorist financing framework.[622]

It is not clear in which way the directive is complementary to the revised FATF Recommendations. For instance, the changes in the Fourth AML Directive represent often a copy of the revised recommendations of the FATF in extension of the scope, including the risked based approach[623] and the non-permission of simplified due diligence or situations where exemptions apply, certainly considering the politically exposed persons [624] as is also the case in the revised FATF recommendations.

6.4.8 Replacement of the Third AML Directive by the Fourth AML Directive

For a better understanding of the Directive, this section discusses the purpose and effects of the Directive, as well as the doubts about the effectiveness of the legislative measures based on these texts and Fourth AMLD, from a privacy perspective.

The leading principle in the Fourth AML Directive is a 'risk-based' approach which takes into consideration that there is an increasing risk, because of the continuously changing technologies. This is enhanced by the unimpeded use of 'alternative' techniques, certainly from the so called 'high-risk' countries. A continuous adaption, meaning extension, of the legal framework is considered indispensable:

The changing nature of money laundering and terrorist financing threats, facilitated by a constant evolution of technology and of the means at the disposal of criminals, requires that quick and continuous adaptations of the legal framework as regards high-risk third countries be made in order to efficiently address existing risks and prevent new ones from arising.

Concerning the use of 'new technologies', the EP in its comment referred to the new technologies in another way keeping in mind the protection of fundamental rights in a new 11th recital added to the proposal of the commission referring to the EU Charter for reference to the fundamental rights. In the definite text of the Fourth Directive this reference disappeared.[625]

---

[622] 4th AML directive, p.3 and recital 4: The measures adopted by the European Union in this field should therefore be consistent with other action undertaken in other international fora. The European Union action should continue to take particular account of the Recommendations of the FATF, which constitutes the foremost international body active in the fight against money laundering and terrorist financing.
Council doc 13 June 13 2014: With the view to reinforce the efficacy of the fight against money laundering and terrorist financing, Directives 2005/60/EC and 2006/70/EC should be aligned with the new FATF Recommendations adopted and expanded in February 2012

[623] The Directive itself further strengthens elements of the revised Recommendations, in particular in relation to scope (by including providers of gambling services and dealers in goods with a threshold of EUR 7 500), beneficial ownership information (which is to be made available to obliged entities and competent authorities), and in the provisions on sanctions, Fourth AML. Also the extension of the revised FATF extension to 'providers of gambling services is copied. Fourth AML Directive, p. 3.

[624] Fourth AML Directive, p. 11.

[625] (19) New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.

Instead the accent for the use of new technologies on proactive risk management was stressed.[626]

The Fourth AML Directive defines as main the objectives of the measures to strengthen the internal market by reducing complexity across borders, to safeguard the interests of society from criminality and terrorist acts, to safeguard the economic prosperity of the European Union by ensuring an efficient business environment, and to contribute to financial stability by protecting the soundness, proper functioning and integrity of the financial system. The text was published as a result of an ample consultation with all relevant stakeholders.[627]

These objectives will be achieved by ensuring consistency between the EU approach and the international one; ensuring consistency between national rules, as well as flexibility in their implementation; ensuring that the rules are risk-focused and adjusted to address new emerging threats.[628]

The EU intends to strengthen the repressive response to money laundering. Consequently it is planned to propose criminal law harmonisation for this offence based on Article 83(1) of the Treaty on the Functioning of the European Union (TFEU) as made clear in the first recital.[629]

The Directive aims to prevent the financial system from being used for money laundering and terrorist financing, and repeals the former Directive, mainly to get the Directive in line with the frequently revised FATF standards and recommendations, as stated in recital 4 of the Directive.[630] Defining the concerned group of individuals was also considered a problem, but

---

[626] *11b) Technological progress has provided tools which enable obliged entities to verify the identity of their customers when certain transactions occur. Such technological improvements provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities of Member States and obliged entities should be proactive in combating new and innovative ways of money laundering, while respecting fundamental rights, including the right to privacy and data protection* Compared to: P. 17 of the EP report.

[627] In April 2012, the Commission adopted a report on the application of the Third AMLD, and solicited comments from all stakeholders on its considerations. In particular, the report focused on a number of identified key themes (including application of a risk-based approach, extending the scope of the existing framework, adjusting the approach to customer due diligence, clarifying reporting obligations and supervisory powers, enhancing FIUs co-operation etc.), which are central to the review of the Third AML. (commission staff working document impact assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial systems for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds, 08-02-2013 6230/13 ADD 1, (2013/0024 (COD) 2013/0025 (COD). Available at: <http://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vj725dcy4fzm>.

[628] In addition, the fourth AML Directive incorporates and ammends Regulation (EU) No 648/2012 of theEuropean Parliament and of the Council, and repeals Directive 2005/60/EC of the European Parliament of the Council and Commission and repeals Commission Directive 2006/70/EC of 1August 2006 laying down implementing measures for Directive 2005/60/EC1, described as thus improving the comprehensibility and accessibility of the anti-money laundering (AML) legislative framework for all stakeholders.

[629] (1) Flows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorism financing and organised crime remain significant problems which should be addressed at Union level. In addition to further developing the criminal law approach at Union level, targeted and proportionate prevention of the use of the financial system for the purposes of money laundering and terrorist financing is indispensable and can produce complementary results.

[630] Union action should continue to take particular account of the FATF Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing. With a view to reinforcing the efficacy of the fight against money laundering and terrorist financing, the relevant Union legal acts should, where appropriate, be aligned with the International Standards on Combating Money Laundering

not from a personal data protection perspective. Of course this directive, as well as its predecessor, aims to prevent the use of the financial system for the purpose of money laundering and terrorist financing. It further applies to financial and credit institutions, as well as to certain legal and natural persons working in the financial sector, including providers of goods (when payments are made in cash in excess of EUR10 000 (proposal 7500)). These entities and persons have to apply customer due diligence (CDD), taking into account the risk of money laundering and terrorist financing. National financial intelligence units (FIU) are set up to deal with suspicious transaction reports (STR's).[631] The final text extends the scope of application to any person or entity that is considered a risk concerning ML or TF.[632] This 'risk-based' approach can extend even further. To prohibit money laundering and the financing of terrorism, the Member States may adopt or retain in force stricter provisions than provided for in this directive.[633]

The conscience of the actions for the Member States is secured in the final recital where a strong reference to the fundamental rights in the Charter is made, covering all activities in the Directive.[634]

6.4.8.1 Definition of Money Laundering and the Financing of Terrorism[635]

The Fourth AML Directive describes money laundering as the following conduct, when committed intentionally:

(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;

(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;

---

and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations').

[631] Available at: <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24016a_en.htm>.

[632] Article 4:1. Member States shall, in accordance with the risk-based approach, ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the obliged entities referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.

[633] Article 5. The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing(…).

[634] (65) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

[635] The following section is derived from the(actualised) report for the FP 7 Hemolia project written by the author.

And, (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).

There seems to be even an EU extended jurisdiction to this 'universal crime'. Money laundering must be regarded as such, even if the activities that generated the laundered property were carried out in another EU or non-EU country.

By 'terrorist financing' the directive means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should 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 such as hostage taking, the drawing-up of false administrative documents and the leadership of a terrorist group or any terrorist or terrorist enhancing activity.[636] The Directive further applies to any finance related offence activity and all tax offences punishable by deprivation of liberty or a detention order for a minimum of more than six months.

6.4.8.2 Obligations of Covered Entities and Persons Vis-à-Vis their Customers

The directive applies to credit and financial institutions, independent legal professionals, notaries, accountants, auditors, tax advisors, real estate agents, casinos, trust and company service providers, and all providers of goods (when payments are made in cash in excess of EUR 10 000. The entities and persons covered by the directive are required to apply customer due diligence measures when establishing a business relationship and when carrying out occasional transactions amounting to EUR 10 000 or more. Furthermore, they must file a suspicious transaction report when there is suspicion of money laundering or terrorist financing, regardless of any exemption or threshold. In these cases there is even the possibility to lower the threshold under EUR 10 000 for Member States or apply other conditions. Furthermore, countries can choose to avoid thresholds in the case of secure electronic payments systems. This extra possibility, understandable from the perspective of sovereignty of the states cannot be understood from a harmonizing purpose.[637] Also from the perspective of legal certainty for the citizens this could create risks in the sense of uncertainty.

The due diligence measures involve identifying the customer and verifying his/her identity, obtaining information on the purpose and intended nature of the business relationship and, where appropriate, identifying and verifying the identity of the natural person owning or controlling the legal entity or on whose behalf the activity is carried out. The extent of such measures may be determined on a risk-based approach depending, for example, on the type of customer or business relationship. EU countries may allow the entities and persons covered by the directive to call on third parties to execute the customer due diligence measures. The directive also lists cases in which simplified customer due diligence measures may be used, such as in relation to national public authorities, customers with life insurance policies with an annual premium of no more than EUR 1 000, or electronic money holders. This list has been minimized in the fourth Directive so more parties and transactions can be considered

[636] 2002/475/JHA15, as amended by Council Framework Decision 2008/919/JHA.5. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 2 and 4 may be inferred from objective factual circumstances. See also: Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, <http://bit.ly/1nYIuX0>.

[637] Member States should be able to adopt lower thresholds, additional general limitations to the use of cash and further stricter provisions. Fourth AML, Recital 6.

suspicious. It is doubtful if this tightening of measures will be successful. Stricter regulations are not a guarantee for success as also is recognized in the assessment report where it is stated that States would benefit from better enforcement systems and not necessarily from stricter rules, even if those rules are considered robust and dissuasive.

Where there is a high risk of money laundering or terrorist financing, the entities and persons covered by the directive are required to apply enhanced customer due diligence**.** Enhanced customer due diligence involves supplementary measures to verify or certify the documents supplied when the customer has not been physically present for identification purposes.

A special position is provided for lawyers, accountants and notaries giving specialized or legal advice subjected to the obligation of professional secrecy and sanctioned by law. This is also sanctioned in the EU Charter and the ECHR.[638]

It seems superfluous in the recital that these groups of exempted professionals should not be 'taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.'[639] Finally, credit and other financial institutions may not keep anonymous accounts or anonymous passbooks.

European countries are required to inform each other and the European Supervisory Authorities (ESA) whether they believe that a third country meets the equivalence conditions concerning the assessment of situations which represent a low risk of money laundering and terrorist financing.[640]

6.4.8.3 Establishment of a Financial Intelligence Unit (FIU) in the EU countries

Each EU country must set up an independent financial intelligence unit (FIU) in the form of a central national unit. These units are responsible for receiving, requesting, analysing and disseminating to the competent authorities information concerning potential money laundering or terrorist financing. EU countries must provide their FIU with adequate resources to fulfil its tasks and ensure that it has access to any necessary financial, administrative and law enforcement information.

The purpose of the FIU is quite clearly described in the amended recital 37 of the fourth AML (29 of the third AML Directive)[641]:

[638]There should, however, be exemptions from any obligation to report information obtained before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Recital 9 Fourth AML.
[639]Therefore, legal advice should remain subject to the obligation of professional secrecy, except where the legal professional is taking part in money laundering or terrorist financing, the legal advice is provided for the purposes of money laundering or terrorist financing, or the legal professional knows that the client is seeking legal advice for the purposes of money laundering or terrorist financing. Recital 9, Fourth AML.
[640] See: European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).
[641] All Member States have, or should, set up operationally independent and autonomous FIUs 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. An operationally independent and autonomous FIU should mean that the FIU has the authority and capacity to carry out its functions freely.

It can be considered detrimental to privacy seeing that the reporting obligation is also present without a threshold if the transaction is considered suspicious, where 'suspicious' is not defined. This is even more the case by noting that the addition of the European parliament was skipped out of the COREPER text, referring to the respect for fundamental rights;

It is important that Member States provide FIUs with the necessary resources to ensure that they have full operational capacity to deal with the current challenges posed by money laundering and terrorist financing, while respecting fundamental rights, including the right to privacy and data protection.

The change from 'conduct' to 'perform their tasks' (proposal) carry out its functions in the Fourth Directive to 'carry out its functions', giving the independence of the FIU a more direct meaning is interesting because it increases the independent position of the FIU's[642] The other important aspect is that the parliament strengthened the operational capabilities. This extended responsibility and the fact that no third parties will be involved to permit actions should decrease the risk of informing third parties, faults or abuse. The other interesting remark of the EP is the continuous reference to the respect for privacy and fundamental rights.[643] This is not always found back in the COREPER text and the final text as it is stated in the Fourth Directive but the influence is undeniable there, be it in the final recital.

The entities and persons covered by the directive must file a suspicious transaction report without delay to the FIU when they know or suspect that money laundering or terrorist financing is being or has been committed or attempted. In the meantime, they must refrain from carrying out transactions. At the FIU's request, these entities and persons must furnish all necessary information in accordance with the applicable legislation.

EU countries may decide whether they require independent legal professionals, notaries, auditors, external accountants and tax advisers to inform the FIU of information they receive from or obtain on their clients when ascertaining the legal position of their client or when defending or representing that client in judicial proceedings.

The entities and persons covered by this directive may not reveal to the customer or to other third persons that information has been transmitted to the FIU, except in the case of law enforcement. They must keep documents and supporting or other evidence for at least five years from the end of the business relationship or the carrying-out of the transaction. The Commission promotes coordination between the EU countries' FIUs. The Directive supports exchange of information, and analysed data via the FIU Platform.[644] Member States are required to inform each other and the ESA where they believe that a third country meets the equivalence conditions concerning the prohibition of disclosure, professional secrecy and personal data protection.

[642] From Third AML to Proposal of the Commission and COREPER text.

[643] Report on the 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)0045) – C7-0032/2013 – 2013/0025(COD)).

[644] (55) The EU Financial Intelligence Units' Platform (the 'EU FIUs Platform'), an informal group composed of representatives from FIUs and active since 2006, is used to facilitate cooperation among FIUs and exchange views on cooperation-related issues such as effective cooperation among FIUs and between FIUs and third-country financial intelligence units, joint analysis of cross-border cases and trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

The credit institutions and other financial institutions covered by this Directive shall apply in their branches and majority-owned subsidiaries located in third countries measures at least equivalent to those laid down in this Directive with regard to customer due diligence and record keeping. Member States, the EAS and the Commission are required to inform each other where the legislation of a third country does not permit the application of these measures and coordinated action could be taken to find a solution. In this case, the EAS have the option of drawing up draft regulatory technical standards to specify the type of additional measures and minimum action to be taken by credit and financial institutions.

6.4.8.4 Enforcement of the Directive and Imposition of Sanctions

As also was required by the FATF, the entities and persons covered by the Directive must establish appropriate measures and procedures for customer due diligence, reporting of information, record keeping, risk management and communication. They must ensure that the relevant employees are aware of the provisions in force.

EU countries must monitor compliance with the directive. The entities and persons concerned must be held liable for any failure to comply with the national provisions adopted pursuant to the directive. The penalties must be effective, proportionate and dissuasive.[645]

6.4.9 The Privacy and Data Protection Aspect

The Fourth AMLD, with respect to data protection, states that the proposed clarifications to the Third AML are fully in line with the approach set out in the Commission's proposals and policy for the data protection framework proposals. Of course a specific provision empowers EU or national legislation to restrict the scope of the obligations and rights provided for in the draft regulation on a number of specified grounds, including the prevention, investigation, detection and prosecution of criminal offences, including money laundering. In the proposed directive there are references to the application of general data protection legislation but no specific clauses or references are made for measures to protect the data of individuals concerned. In the proposal the need to strike a balance between allowing robust systems and controls and preventative measures against money laundering and terrorist financing on one hand and protecting the rights of data subjects on the other is reflected.[646] Further the measures should be purpose-orientated and take into account the subsidiarity and proportionality principle. Still, the EP has added many references to the protection of fundamental rights and privacy as defined in the European Charter in the considerations and articles of the proposed directive.

The applicability of the data protection directive (Directive 95/46/EC) is confirmed in recital 420. How this is meant is made clear in the following paragraphs of this consideration in the COREPER text.

'The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. This Directive is without prejudice to the

[645] Available at: <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l24016a_en.htm>.

[646] (33) This Directive is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including the provisions of Framework decision 977/2008/JHA, as implemented in national law.

protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including Council Framework Decision 2008/977/JHA (3), as implemented in national law;'

In other words, exemptions from this protection are found in the public interest and are therefore possible. The next step in consideration is to make clear that

'the fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States.'

This is an accepted ground to limit the application of the Data Protection Directive. Public interest and anti-criminal investigations are also here well recognized principles to limit the protection of privacy of natural persons.

The European Banking Industrial Committee (EBIC) agrees with this point of view but also seems to agree upon the fact that also data protection can be considered of public interest.[647]

The main attention of the directive concerning privacy was given in the amended consideration 35 of the European Parliament where the purpose, the limits and the respect for privacy was made clear. Although this text has disappeared in the Council document, the common limitation principle in this text restricted the essence of privacy protection.[648]

For the sake of the purpose of the investigation and prosecution, the right of access of the subject is limited (r. 34/35). In general though, the rights as defined in the ECHR and the Charter have to be respected although in line with the FATF rules

'It is essential that the alignment of this Directive with the FATF Recommendations is carried out in full compliance with Union law, especially as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (Charter)'.[649]

---

[647] *EBIC welcomes the recognition by the European Parliament in its amendment to Article 40a that "the collection, processing and transfer of information for anti-money laundering purposes shall be considered to be a matter of public interest under Directive 95/46/EC." This provision should be maintained in the final compromise text and shall be without prejudice for (national) competent authorities to define purposes other than the prevention of money-laundering as 'matter of public interest' as per data protection legislation.* Position paper 4thAML EBIC, http://bit.ly/1zWf0Ba.

[648] EUROPEAN UNION Brussels, 13 June 2014 (OR. en) Interinstitutional File: 2013/0025 (COD) 10970/14.

[649] 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. In particular, further processing of personal data for commercial purposes should be strictly prohibited. R. 43.

This means that the application of the Charter will only be valid outside the scope of the Directive. Limitation of these rights is also a right (for the state). Storage of the data can be extended from 5 to 10 years when deemed necessary.[650]

In the former text, added by the EP, the Parliament asked for counterbalances by an effective and credible data protection authority and at least transparency and investigative powers when the procedure is questionable. Still there is understanding for the purpose of the Directive as such anti money laundering and counter terrorism financing.The actual text of the directive underlines the exception to the 'normal' protection of personal data:

(46 former 34) The rights of access of the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to information contained in a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Limitations to this right in accordance with the rules laid down in Article 13 of Directive 95/46/EC may therefore be justified.

In the amendments of the Parliament, the text continued as follows:

However, such limitations have to be counterbalanced by the effective powers granted to the data protection authorities, including indirect access powers, laid down in Directive 95/46/EC, enabling them to investigate, either ex officio or on the basis of a complaint, any claims concerning problems with personal data processing. This should in particular include access to the data file at the obliged entity.

In the final text of the Council this addition has disappeared and partially returned in the COREPER text where at least a suggestion for independent control is made:

The data subject has the right to request that a supervisory authority referred to in Article 28 of Directive 95/46/EC or, where applicable, the European Data Protection Supervisor, checks the lawfulness of the processing, as well as the right to seek a judicial remedy referred to in Article 22 of Directive EC 95/46. The supervisory authority referred to in art. 28 of Directive 95/46/EC may also act on an ex-officio basis. Without prejudice to the restrictions to the right to access, the supervisory authority should be able to inform the data subject that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.[651]

In the final text of the Directive replacing the COREPER text there are not many changes except for the introduction as kind of warning not to lose the purpose of the Directive in Recital 46.

The right of access though, can only be executed by the subject if he was aware of the fact that he is suspect in a suspicious transaction. This, probably will not be the case often, referring to the first part of R.46.

The respect for fundamental rights is accentuated in general terms but was also specified to some very important fundamental legal principles such as the presumption of innocence, in effect leading to the conclusion that a claim of suspicion does not automatically include a

[650] Recital 31 a COREPER text.
[651] Recital 34 COREPER text, r.33 has disappeared completely.

reason for intrusion of privacy to fight ML. The subjects of an investigation may presume a balanced and proportional reaction by the investigative authorities, as proposed by the European Parliament,

(46) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular, the respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence, the rights of the defence.

The reference to the presumption of innocence has disappeared from the final Council text, reappeared in the COREPER text. The general reference to the fundamental rights as cited in Recital 48 had disappeared:

(*48) This Directive respects the fundamental rights and observes the principles recognized in particular by the Charter of Fundamental Rights of the European Union. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the European Convention on Human Rights.*

Instead, this was replaced with the following in the COREPER text:

(48b) The European Data Protection Supervisor delivered an opinion on 4 July 2013

The final text is more directed toward the functional application and harmonisation of AML measures within the Member States without too much specification for privacy principles in the different Articles. FATF recommendations are leading.

The former important specification of reference to the fundamental rights and specifically the Charter reappeared in the final text of the Directive in Recital 65:

(65) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

With the view to reinforce the efficiency of the fight against money laundering and terrorist financing, Directives 2005/60/EC and 2006/70/EC should, where appropriate, be aligned with the new FATF Recommendations adopted and expanded in February 2012.

Further, a reference to the principles of transfer of data to third countries outside the EU is made in the spirit of the principle of the minimum standard of protection on the European level. In general, it is a leading principle that information is not disclosed to the persons to whom the measures are concerned, against whom the investigation is proceeding or with regard to any other requirement applied that is deemed necessary by the concerned authorities. As stated above, this is understandable, but principles for informing the data subjects afterwards and informing them about remedies should be in place, even if the subject was not aware of the inquiries.

Article 28 of the First AML proposal used to refer to the fact that disclosure of the information to and from authorities is allowed as long as it is in accordance with legal data protection

legislation. Besides the fact that the human rights legislation, as well as the data protection legislation, gives ample opportunity to limit the application of the full data protection principles, article 28 in this sense was skipped all together in the council text, and was replaced by article 38 in the COREPER text without any reference to privacy protection principles. In Article 41of the final text of the Fourth AML Directive the application of the general privacy Directive is confirmed only to be followed by the conclusion in Article 43 that the exception of public interest is applicable to this Directive.[652] The disclosure and exchange of personal data as also referred to in the FATF recommendations, will undoubtedly always be supported by law. The question is, in the light of the European Courts ruling on the retention directive, if limitation on the basis of this AML Directive is considered legitimate with enough guarantees as mentioned in the ruling concerning proportionality and independent control. One could argue that there are not enough guarantees to legitimize the intrusions on privacy given that the reference to data protection is made in a peculiar manner, only referring to the fact that the subject of the Fourth AML Directive is a matter of public interest. This is even more questionable given the fact that actions of the inquiring authorities, including the FIU's are based on the vague 'Risk Based Approach'.

6.4.10 Risk-Based Approach

The main orientation of the evaluation report of the Third Directive is integration with international standards adopted by FATF.[653] The purpose of the evaluation, according to the evaluation report of the Commission, is to restructure the legislation on the basis of: a number of identified key themes, which are central to the Third AMLD's objectives. Under each theme, a recital is given as to how the existing rules have been applied, which factors may drive changes (in particular resulting from the international revision process), and what the possible options for changing the existing EU rules might be.

Crucial in evaluation and addition for the 'new' Fourth AML Directive is considered a risk-based approach that enables a more targeted and focused approach to assessing risks and applying resources to where they are most needed. That means that a more harmonized but also more specified procedure is recognized by the Commission as well as by the Member States:

RBA applied by FIs and Designated Non-Financial Businesses and Professions (DNFBPs): explicitly introducing a requirement that risk-based procedures designed by obliged entities are appropriate to the size and nature of the entity, and have to be documented, updated and available to competent authorities.[654]

This RBA is clearly copied from the FATF recommendations framework that is strongly risk base oriented. It is considered by the FATF as an effective way to combat money laundering

[652] 1.The processing of personal data under this Directive is subject to Directive 95/46/EC, as transposed intonational law. Personal data that is processed pursuant to this Directive by the Commission or by the ESAs issubject to Regulation (EC) No 45/2001 and Article 43: The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Directive 95/46/EC.

[653] Report from the Commission to the European Parliament and the Council on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, Brussels, 11 April 2012 COM(2012) 168 final (3rd AML directive evaluation report).

[654] 3rd AML directive evaluation report, p. 4. Further, Article 34 of the Directive requires obliged persons and institutions to establish 'adequate and appropriate' AML/CFT(Countering the Financing of Terrorism) risk management policies and procedures.

and terrorist financing. There seems to be a strong inclination to approve an 'application creep' of the RBA concept in extending its appliance to other sectors, legal and natural persons without too much motivation or even explanation.

The offence of money laundering (Article 1(2)) is committed when the proceeds of 'criminal activity' are laundered. Article 3(5) sets out a range of 'serious crimes' that are considered to be criminal activities. Beyond the listed offences, the Directive takes a general approach with respect to all other offences which carry a punishment of imprisonment based on a mixture of maximum and minimum thresholds.

In the final text of the Directive in Article 2.7 there are several open ended possibilities to extend the activities to non-specified potential risks:

In assessing the risk of money laundering or terrorist financing for the purposes of this Article, Member States shall pay particular attention to any financial activity which is considered to be particularly likely, by its nature, to be used or abused for the purposes of money laundering or terrorist financing.

The fact that 'Risk based is leading' creates open end investigative powers and data processing as long as it is considered within the scope of the Directive:

R.(22) The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk- based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.

This leads to the text of Article 8 where a very general obligation for the Member States is described refering to identification and assessment of risks on their own estimation dependent on all possible circumstances.[655]

Moreover, the FATF list includes tax offences, broadening the list. For instance: is a wrongfully applied electronic form considered a tax offence, and what are the thresholds for the offences? Also the subjects that are covered will be extended according to the document. Online casinos were already on the list but also all other gambling activities, yet including all electronic gambling; real estate offices, including letting; handlers in precious stones and metals and of course all traditional financial institutions have to be scrutinized in the new legislation. Low risk activities may be exempted on a national decision basis.

Certainly the extensions to the internet activities is understandable but it is practically quite impossible to control, let alone manage the immense administrative burden for the (non-existing rules) reporting parties and the increasing workload for the FIU's. Naturally, there is a risk of mistakes concerning the legal transactions of innocent legal subjects. With the increased immense number of transactions to be reported, the risk certainly will increase.

[655] *Article 8* 1.Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.

Apart from the broadening of the application of the directive as a rather questionable action (be it that exceptions are possible under Article 2(3) of the Third AML Directive and proposals), the extension of the scope also has large administrative repercussions. This is even more so because of the recitals that are given to the proposed lowering of financial transaction limits.[656] Additionally, the position of politically exposed persons has been under 'reconstruction'. Surprisingly, some Member States consider the definition in the directive too broad, covering also family and close associates. Still this extension has been accepted in the final text.[657]

The consciousness about the open ended construction of RBA forced the Commission to draw up a riskbase assessment report in June 2017 on a Union level and report on these developments every two years from that day on.[658]

6.4.11 Personal Data Protection within FIU Exchange

The backbone of the cooperation between the FIUs is based around a Council Decision dating back to 2000.[659] In the evaluation report it is recognized by the different stake holders that a better interaction between AML and personal data protection obligations has to be ensured. Already in a study carried out in 2008 by the FIU-Platform, a solution had to be sought to identify possible convergence points as well as areas where difficulties might need to be reconciled between the respective legislation.[660] The study was more directed to remove limitations to exchange personal data and use the data for further investigations. The study was not seeking an acceptable equilibrium by stressing the need for the protection of personal data with reference to proportionality and purpose orientation.

The possibility to use also sensitive personal data is to be found in the exemptions to the rule on basis of:

the principle of processing sensitive/specific data for reasons of substantial public interest (Directive) or when this is strictly necessary (Framework Decision) and when appropriate safeguards are provided for by national law.

The general principle of Article 8 ECHR is not mentioned in the report. Reference is just made to the Data Protection Directive which seem to be a bit limited to defend the positioning of the platform. The view of the platform is that the reporting party should be protected instead, on the basis of integrity and confidentiality:

---

[656] (i) Reducing the EUR 15 000 threshold in Article 7(b) in respect of occasional transactions; (ii) Reducing the EUR 1000 threshold for electronic fund transfers in Regulation 1781/2006; Third AML Directive evaluation, p. 6.

[657] Article 3(10): 'family members' includes the following: (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; (b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person; (c) the parents of a politically exposed person; 5.6.2015 L 141/87 Official Journal of the European Union EN.

[658] Article 6.1.The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

[659] Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.

[660] Report on Confidentiality and data protection in the activity of FIUs. Available at: <http://ec.europa.eu/internal_market/company/financialcrime/index_en.htm#fiu-report-money>.

The report of suspected of money laundering or terrorism financing to the intelligence unit benefits from a very high level of confidentiality arising in particularfrom a wish to ensure the protection of the identity of the reporting party and avoid the latter becoming the victim of attacks or reprisals.

In the fourth AML assessment report, reference is made to the impact of the proposal to fundamental rights. The report stresses that the proposal will help to protect the fundamental right to life (Article 2 of the Charter) which is threatened by criminal activities and terrorism. The Charter also recognizes as a fundamental right the protection of private life and personal data (Articles 7 and 8 of the Charter). Therefore a direct reference to Article 52 of the Charter is made, which recognizes that some limitations to fundamental rights may be laid down by law if proportionate and necessary, for example to protect common good, or fundamental rights and liberties of other people. Although an overall acceptance of limiting fundamental rights is accepted, bringing more clarity to the subjects is considered by specifying the conditions to retain or process data:

The proposal should also reinforce fundamental rights by bringing clarification on how institutions need to apply AML/CFT requirements in a way which is compatible with a high level of protection of data, in comparison to the current situation where legal uncertainties can lead to inefficient outcomes (i.e. as regards their degree of protection of data). As an example, by specifying the conditions under which data can be retained, protection of data subjects will be strengthened.[661]

But how can this admirable objective be reached by the Fourth AML Directive? Without too much optimism three possibilities are presented in a scheme that is presented in the assessment report considering data protection regarding data retention and interchange between the user groups (LEA's and FIU's).[662]

Firstly, the option is given not to change anything. The conclusion is that this option would lead to still continuing legal uncertainties and practical difficulties. This is unacceptable. The second option is, in my opinion, a condition sine qua non to arrive at the third phase. The third option is in line with the advice of the Article 29 Working Party and the proposals for the new European framework for data protection. Not just from a data protection perspective but also from an aspect of functionality it is necessary to improve the clarity as well as harmonization of the legislative requirements among the 28 Member States.

Policy options	Comparison criteria		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0
	0	0	0

[661] Commission staff working document impact assessment. Accompanying the document 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, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds {COM(2013) 44} {COM(2013) 45} {SWD(2013) 22}.
[662] Assessment report, 3rd part of scheme 12, p. 104.

2. Require MS to clarify interaction between AML/CFT and DP rules at national **level**	+ Reduced uncertainties for entities; better compliance with AML and data protection requirements + Enhanced level of respect of data protection rules + In line with Operational Objectives 1 and 3	+ Member State authorities would retain flexibility	
	- Incoherence across Member States		- Not in line with Internal Market
3. Introduce new rules in the AML Directive to clarify interaction, in particular as regards data retention and data sharing within the groups	+ Enhanced coherence across Member States; + Reduced uncertainties for entities; better compliance with AML and data protection requirements + AML group-wide compliance facilitated + In line with all Operational Objectives	+ Cost savings for groups	+ In line with Internal Market + In line with International Standards + In line with Commission's Data protection proposals
	- Data sharing with third countries whose DP regimes have not been recognised likely to remain problematic	- Possibly difficult to agree on a wording which reflects an appropriate balance between AML and DP objectives	

In the third option new regulations will decrease the existing uncertainties according to the assessment report:

New provisions might clarify how long data can be held by obliged entities, the circumstances under which data can be transferred to third countries, and ensure that data collected for AML/CFT purposes cannot be processed for commercial purposes.[663]

The mentioned risks and the fact that the interests as well as the translation of definitions will be difficult to ascertain in a harmonized way. This problem will certainly remain as is mentioned in the assessment. Certainly the data protection regimes and retention regulations will vary amongst the European Member States. Therefore it is not only necessary to get AML regulations on one line but also data retention rules and data protection regulations as well. The problems are indicated by a ruling on the obligation to exchange data. The problematic issue of compliance is indicated by the Court ruling on a preliminary question in Case C-212/11 from the supreme Spanish Court (Tribunal Supremo (Spain) (Jyske Bank Gibraltar Ltd v. Administración del Estado). In paragraph 53 it is clarified as follows:

[663] Assessment report, p. 105.

'In that regard, it should be noted, first of all, that, whilst Directive 2005/60 lays down numerous concrete and detailed requirements on customer due diligence, on disclosure and keeping of records, which the Member States must impose on the financial institutions covered, it does not, concerning cooperation between the FIUs, itself lay down any requirements or procedures, but merely states, in Article 38, that the 'Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community'.[664]

6.4.12 The Problem of Inconsistencies

The problem, as also noted with the retention directive and leading to its demise, is the disharmonized application within the Member States. This is often inherent to the fact that a directive gives ample opportunity to apply the rules in a way suitable to the different legal culture of that State on basis of the subsidiarity principle. European regulations should only regulate the matters that cannot be regulated by the states themselves. In this case this results in a European patchwork blanket that, instead of harmonization of procedures and definitions, and creates a pick and choose European framework. This results in differences in reporting, access, storing of data as well in defining the cases where reporting is required. The interchange of data between the requesting European partners therefore creates an incomparable set of data that easily can result in undesirable suppositions for prosecution.[665]

In the report of work carried out by Eurostat and DG Home Affairs by Cynthia Tavares and Geoffrey Thomas, this leads to the observation that the reporting data seems to be quite incomparable, ironically referenced to as 'flexibility':

'Article 5 of the Third Anti-Money Laundering Directive authorises Member States, in accordance with the principle of subsidiarity, to lay down measures which go beyond the obligations required by the Directive. This allows for a degree of flexibility, as can be seen in the adoption of different concepts when implementing the Third Directive. Whilst the Suspicious Transaction Report – STR- is the counting unit most used by Member States, some (United Kingdom, Cyprus and Finland) have preferred to use the Suspicious Activity Report - SAR. The Netherlands has preferred to use a different concept in the form of the Unusual Transaction Report - UTR.'

The use of different counting units, each with a different scope, inevitably compromises the comparability of data between Member States. Moreover, it would be pointless to compare the absolute number of such reports without looking to correlate figures in relative terms, that is to say by comparing them with the size of the financial sector of each Member State .[666]

In the report of the FIU Platform a number of shortcomings with the existing legislation is recognized; the cooperation on terrorist financing is not foreseen in the Decision. There are difficulties for FIU's to cooperate because there are different interpretations of the legal basis, referring to the Decision to undertake specific types of cooperation, such as the automatic

[664] Supreme Court (Spain) 25 April 2013, Jyske Bank Gibraltar Ltd v. Administración del Estado, [2013] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62011CJ0212:EN:HTML
[665] C. Taveres, G. Thomas & M. Roudaut, *Money laundering in Europe. Report of work carried out by Eurostat and DG Home Affairs*, Luxembourg: Publications Office of the European Union 2010.
[666] Tavares, p.13

exchange of information when links are found with another Member State. Some of the problems in exchanging information stem from the different powers that FIUs have at national level, including the possibility to access information. Some of the FIUs have investigative powers and others just have administrative status to combine the information and leave the investigations to the police after filing the Suspicious Transfer Report (STR). Also the fact that no actions are available before filing an STR is considered a problem. This is considered a main problem by the platform but from a data protection point of view these competences to investigate without a sound legal basis would be against the most essential legal certainties anyway.

Also the platform utters the wish that the data should be treated like data from judicial data files, including data from files that were closed by FIUs. This could result in the exemption as is the case in most law systems that these data are considered 'police data' and in most national legal systems, could be used and stored for undefined periods of time.

Also mentioned in the paragraphs on retention,[667] the question of reconciling different storage periods is posed within the framework of operational cooperation between FIUs. Within the platform report the question was posed if the period applicable with respect to retention of personal data should be that of the country of origin of the sent information or the period applicable in the receiving country.

The different storage periods and the indiscriminate types of data in the different Member States causes legal uncertainty as well as problems in the validation of the data by the financial and investigative authorities. This is well illustrated by the interpretation of the Platform referring to the formerly discussed proposal on the Data Protection Directive on police matters of the data protection framework where:

'the transmitting authority may upon transmission indicate the time limits for the retention of data, following the expiry of which the recipient must also erase or block the data or review whether or not they are still needed. This obligation shall not apply if, when these time limits expire, the data are required for a current investigation or prosecution. When the transmitting authority refrained from indicating a time limit, the time limits for the retention of data provided for under the national law of the receiving Member States shall apply.'[668]

Another risk that is considered an 'investigative difficulty' is that an individual can be the object of successive reports submitted to the FIU, which poses the problem of defining the start date for the data storage period. The solution that is proposed by the platform is that:

'considering the fluctuating nature of the data that FIUs are expected to process, it would be suitable for their data storage period to begin when a new piece of information is communicated to them about the person concerned'.

This again results in an escape clause to lengthen the storage period for an indiscriminate period of time. In the Platform's perspective there is a clear danger of 'short-sightedness' to the problem of hindrances to the use and the exchange of personal data for further investigation and AML activities where the Platform concluded that:

[667] Paragraph 5.3.5.
[668] FIU platform report, p. 7.

'the interaction of AML rules with national data protection rules appeared to be a main factor impacting bank's AML policies at group level and hindering effective intra-group transfer of information.'

6.4.13 Concluding Remarks on AML Regulations

To conclude with the main problems and inconsistencies in the field of AML legislation and retention, there still is a variety in definitions and a variety in legal competences, institutions and authorities, not just among FIU's but also concerning the investigative competences of the police on basis of the qualification of the alleged crime or suspicion of crime. On top of that there is a difference in definition of suspicious transactions amongst the Member States. Some Member States report on the activities of the subject on the basis of 'unusual' transactions and other report these as 'suspicious' transactions. This is also connected to the definitions of the activities of the data subjects and the alleged crime. As is the case of the retention directive concerning telecommunication traffic data, also in AML regulations, differences exist in the legal retention period. This extends as well to the applicability to different types of data (internet versus telecommunication or telephone data, missed calls etc.), procedures and security measures as to the periods of retaining the personal data.

'*a wide diversity of national measures can complicate cross-border compliance, and lack of practical guidance available.'*[669]

Also in the earlier text of the Fourth AML directive, the difficulties and disharmonisation of the (legal) sanctions are acknowledged wherein,

'Member States currently have a diverse range of administrative measures and sanctions for breaches of the key preventative measures. The diversity could be detrimental to the efforts put in combating money laundering and terrorist financing and the Union's response is at risk of being fragmented'.[670]

In the final text of the Fourth AML Directive this conclusion has led to Recital where it is stated that detailed rules for the FIU's are specified[671]. But the fact is that we have to wait until 2017 to have clear guidelines on the scope of Risk based Approach and consequential effects.[672]

Tavares rightfully attributes this to the open-ended structure of the use of the directive as legal instrument with a strong emphasis on the national subsidiarity principle within financial and national security issues:

---

[670] COM(2013) 45 final, Interinstitutional File: 2013/0025 (COD) R. 41.

[671] (54) Taking into account the transnational nature of money laundering and terrorist financing, coordination and cooperation between FIUs are extremely important. In order to improve such coordination and cooperation, and, in particular, to ensure that suspicious transaction reports reach the FIU of the Member State where the report would be of most use, detailed rules are laid down in this Directive.

[672] 10.By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 on the characteristics of a risk- based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down. *SECTION.*

'This flexibility arising from the application of the principle of subsidiarity and the use of a directive is again evident in the operational choices made by the Member States.
Each Member State is free to determine the approach in the fight against money laundering in a way consistent with the obligations in force. Consequently, each Member State has made different operational choices'[673]

The differences in competences, availability and access to different databases are collected in a questionnaire that has been sent out to the different European FIU's in 2012 in the European FP7 research project HEMOLIA and is presented on the HEMOLIA site and in annex to this thesis.[674] As can be seen, there is a tremendous difference in competences, access to different databases and formulation of suspiciousness of the reports. On top of that it is not reflected in these reports that the reporting entities also vary in reporting to the FIU's what they consider suspicious transactions. Some of the countries consider certain transactions suspicious that are not considered so by other European countries.

To illuminate the opaque situation there is a considerable variety in considerations and explanations by EU, CoE, FIU Platform, FATF, and WP29 among others, on their vision of the AML directive. The orientation is so diverse that there is a severe risk that a definitive acceptable and realistic EU Fourth AML Directive will still have an open ended structure as is proven in the final text. Also proposals to reduce the financial and functional control threshold will create massive administrative problems as well as a bigger risk for the data subjects to be considered as carrying out a 'suspicious transaction'.

Many of the doubts from a personal data protection perspective are also to be found in the June 2011 Article 29 Working Party on Data Protection when it issued its 'Opinion 14/2011.'[675] The Opinion addressed the interaction between AML and personal data protection provisions at a much wider level than the mere transfer of information, and calls for more detailed consideration of DP issues in the AML/CFT legislation to provide for effective data protection compliance. The Working Party addresses no less than 44 recommendations. They should be discussed in more detail in combination with all important recommendations and principles that should be applied in order to obtain a clear and legally acceptable balance between the fundamental right to privacy as defined in Article 8.1 of the ECHR and the possible limitation of this right under paragraph 2 of that Article.

'Hence, measures that are imposed as obligations to prevent money laundering and terrorist financing should always have a clear legal basis and remain necessary and proportionate to the nature of the data. The WP29 recommends i.a. a review of current and proposed AML/CFT laws at EU and national level (rec. 3), more EU harmonization (rec. 5); readable public data protection policies (rec. 12), clear information for visible AML/CFT measures such as questionnaires and the limitation of services (rec. 13), and the strict and clear application of the purpose limitation principle in AML/CFT laws (rec. 15-16).'

The WP29 opinion calls in particular for a balanced way of handling the principles and obligations in this area taking into account the different opinions, interests and legal framework in the EU and international (Human Rights) treaties. Furthermore, privacy and data protection

[673] Tavares, p.13.
[674] This report was delivered by the WP 1 of the Hemolia project in March 2012.
[675] Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, 01008/2011/EN WP 186. Available at:
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp186_en.pdf>.

rights and obligations should always be addressed and developed in this area *in a positive way*, rather than referring to privacy and data protection as an obstruction to AML and ATF activities by the addressed authorities as worded as such by the FIU Platform opinion. There is also caution against the use of

'blanket application of exceptions to data protection legislation, ignoring the conditions for such exceptions', and offering in return no real content and substance to privacy and data protection in the context of AML/CFT processing.'

To have an acceptable AML policy in line with the aforementioned developments in the data protection field, more detailed provisions need to be taken into account. Among other things, the principles for personal data processing, to grant a legal basis both for such processing and for the proportionate restriction of the rights of the data subject when necessary to achieve the goals of the AML/CFT Directive, need adequate safeguards and consistency with the data protection acquis. In addition, consideration could be given to fostering further interaction between AML regulators and data protection supervisory authorities to reach a balanced application of the rules.[676] This opinion is echoed by the European Data Protection Supervisor in 2012.[677]

6.5 Conclusion

In this Chapter the anti-terrorism and financial supervisory regimes from several inter-governmental organizations are described. The regulatory framework spans the fight against terrorism and the supporting actions, specifically ML as well as legislation that provided for the limitation of possible protection of fundamental rights in this perspective.

It is well recognised that terrorism and the financing of terrorism pose a serious threat to security and public wellbeing. Regulatory instruments are imposed on different levels to counter terrorist- and supportive activities. All those legislative instruments in one way or another give opportunity to limit these rights of natural persons if circumstances require so.

The question raised at the outset of this chapter was:

Are the measures initiated by international governmental organisations and non-governmental fora to control and counter terrorist and other illegitimate activities and (financial) support in particular considering the anti-terrorism acts, and, anti-money laundering regulation and procedures compatible with the fundamental right of data protection and privacy?

The main problems are to be found in the impossible task to define the scope of Risk Based Management and to harmonise definitions on a national level and create consistency in terms and regulations. Authorities aim to control data and financial transactions and as a consequence

[676] Report from the Commission to the European Parliament and the Council on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, Brussels, 11 April 2012 COM (2012) 168 final.

[677] *'The growing trend to acknowledge the importance of data protection in proposals for legislation is a welcome one. But on closer examination, the claims are often not supported with concrete measures and safeguards. A lack of further details will also result in undue discrepancies among Member States. Data protection should therefore not be perceived as an obstacle to combat money laundering but as a basic requirement necessary to achieve this purpose'.* Giovanni Buttarelli, Assistant EDPS.

fundamental rights as free flow of information, privacy and informational self-determination are progressively more restricted. In the Fourth AML Directive there is still no consistent set of terms and definitions that could harmonise the procedures within the Member States. Still there is the opportunity for Member States to store personal information for five years if it serves AML/CFT purposes. Whether all those measures initiated by international governmental organisations and non-governmental fora to control and counter terrorist and other illegitimate activities and (financial) support are legitimate within the international legal context is hard to decide upon because of the ample competence governments have on this subject. Anti-terrorism acts, and, counter-money laundering regulation and procedures are not very well specified and are often shaped in an open ended way to give room for national competences. The international regulations on fighting terrorism and AML do not excel in specification and transparency considering the possible limitation of privacy. Terrorism and financing thereof is a global issue. On the level of the UN harmonisation of regulations and definitions is an impossible task. The more because the Members are differing in political character and attainment of purpose. Even if the actions are legitimized by law, the outcome should not always hold because of the lack of transparency and sufficient independent control.

If we consider the reporting instruments of suspicious financial actions that can lead to further investigations of the actions of data subjects, we move to numerous differences in policy by the competent authorities in the use of data including personal data.

Although several Court decisions on national as well on international (ECtHR) level have shed some light on the boundaries of the application and execution of the limitations by authorities, by specifying the principles and circumstances under which the limitation is allowed or unjust, new legislation still is contradictory. This chapter showed that there is a clear development to extend the application of AML and ATF regulations and legal descriptions by 'defining' open norms that will give ample opportunity to take investigative action by investigative authorities as law enforcement authorities and other national investigative services as intelligence agencies. On top of that, the possibility to use these crime investigative activities as an excuse to limit the fundamental protection of privacy on basis of the limitation, are facilitated in the national and international legal instruments.

The outcome could be of help for a more privacy oriented evaluation of 'limitation instruments' as the fourth AML directive, the retention legislation and the legislation on Counter Terrorist Measures. This is already recognized by the EP report on the proposal of the Commission, specifically concerning the privacy orientation in a 'risk based construction.'

What is left in the Council Document is a meagre reference in the explanatory document:

'Data Protection: the need to strike a balance between allowing robust systems and controls and preventative measures against money laundering and terrorist financing on the one hand, and protecting the rights of data subjects on the other is reflected in the proposal'.[678]

And an even more strongly motivated explanatory remark on the impact assessment:

'In addition, the impact assessment analysed the impact of the legislative proposals on

[678] Expl doc p.11.

Fundamental Rights. In line with the Charter of Fundamental rights, the proposals seek in particular to ensure protection of personal data (Article 8 of the Charter) by clarifying the conditions under which personal data can be stored and transferred'.[679]

The reasoning of the ECJ concerning the retention directive could well be applied to other intrusive regulations in trying to secure a legitimate and proportional execution of limitations on privacy. The Fourth AML Directive in the Council and the COREPER text is missing reference to proportionality and the specification of purpose as an independent authority basis for control of the applied measures.

[679] Exp. Doc p.8.

7 Conclusion

'That's why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protections to prevent abuse.'
--President Obama, 23 May 2013[680]

This observation by President Obama encompasses the subject of this thesis but also underlines the insecurity of governments to convey that they are making clear decisions and that they are giving transparent rules in balancing the interests of fundamental rights and the common good, in this case national security.

International treaties and national legislation contain general principles that apply to privacy and the processing of personal data. Privacy is a fundamental right, but not an absolute right. This thesis focused on Article 8 of the ECHR. Exceptions to the right of privacy are based on the exception clause of Article 8 (2) and derived legal instruments, which leave room for interpretation. In this thesis the conditions that have to be met are elaborated upon, the framework of exceptions is described, ECHR case law is analysed and EU and national legislation are examined on the basis of the applicable principles and the conditions that govern the exceptions to privacy.

The point of departure has been the integrity of the personal sphere and the reasonable expectation of privacy a natural person may have as a civilian within society. The limitation of privacy by government is generally accepted as 'conditio sine qua non' in modern technology advanced society, in order to fight crime and defend national security.

The question is how far do we as citizens allow governments to go? How can privacy and defending national security be aligned? Indeed defending privacy and national security are both considered essential for the common good, they are not mutually exclusive. Although the responsibility lies with the democratic representation of the peole as for instance advocated by Habermas, the actual credible control mechanism fails to exist in most 'democratic' societies, let alone in less democratic societies.

7.1 Research Outcomes

In answering the questions of this thesis I have consulted the opinions on different scholars from various era's and cultures. Further, I have studied the developments of national and international legislation as well as the Courts decisions on conflicts between the often considered individual right of privacy and the intrusion rules on this right for the 'common' good, often connected to national security. The outcome is open to further discussion.

The general question as presented in Chapter 1 was:

680 The National Security Agency: Missions, Authorities, Oversight and Partnerships, May 2013.

Is it possible to create regulations that will guarantee an acceptable intrusion on privacy under specific circumstances? Are the actual regulations too open-ended? Is government overstepping its competences?

This is not an easy task, given the fact that privacy is not an absolute right and that the intrusions diversify due to the circumstances in political and cultural sense.

Therefore, to answer the question, it must be combined with the logical follow-up questions:

How can one balance the individual's fundamental right of privacy, on the one hand, and the criminal investigation and measures adopted by the state security to protect society on the other hand? Does the existing regulatory framework suffice, and if not, what adaptations are needed?

In Chapter 2 the question was postulated:

How, with respect to the historical context, has the concept of privacy developed and has been evolved to its present contents?

Considering the historical context, the concept of privacy has developed into a dynamic non-absolute right that is permanently changing relating to the actual social and political context of society. The private sphere of seclusion, of non-interference, is gradually changed into a semi-permanent surveillance, be it part of its own choice, be it as an extension of conceived tasks within society and of course the increased technological possibilities.

It has become a sensitive obligation to protect privacy by government on one side as well as to use a governmental instrument in limiting the same right on grounds of other governmental obligations to defend public order and national security on the other side. It seems that development of the state interest as presented by Aristotle (polis) has overwhelmed the individual interest (oikos); but has not that always been the case? The growing complexity of society continuously demands growing, or at least more complex, state apparatus that has to supervise society.

There are some basic principles. As Locke already noted, the government has no sovereignty of its own - it exists to serve the people. Locke sees personal liberty as the key component of a society that works towards the individual's and the commonwealth's best interest. It is commonly accepted that private interests cannot always be represented by the individuals themselves, a positioned shared by Habermas. They have to compose an authority that will represent their interests as a common denominator. In other words, there is always the sovereignty of the individual to decide how far the transfer of rights will stretch.

But should it be accepted, as Carl Schmitt questioned, that it should be the State's prerogative to define where the state would not have to mind about fundamental rights of its citizens? The limits of stretching are based upon constitutions, the European Convention on Human Rights, the Charter of the EU and several other international and national legal instruments. There seems to be an inclination to use the exception in an 'overstretched' manner.

The right to be let alone as a residue of the historical development of privacy as the sovereignty over one's personal life and information has changed into a right of control over one's information. This control lies for a part within the sovereignty of the individual and for an

increasing part within the sphere of third parties, specially commercial and governmental institutions. Sometimes the control is willingly transferred to these institutions by the individual subject but the access and control of the quantity, quality and content as the core subject of privacy is increasingly harder to execute by the individuals. The laws and regulations that would provide for these controls are difficult to grasp for the subjects and the control by the institutions to legally limit purpose, proportionality of using facts of personal life and information to safeguard privacy is an even hard task. This is all the more difficult if political pressure to extend the limits of processing personal information is justified by reasons of fighting crime and terrorism in order to protect national security and the manage the vulnerability of a democratically controlled nation. Still there is the political responsibility of the sum of individuals as stated by Habermas. Ultimately this can result in a system where the control, by courts and parliament, result in a determination of informational sovereignty as ascertainment in the democratic society. This clearly was the evolution in Gemany by evolving informational self determination from the basic right of individual sovereignty in the constitution.

In Chapter 3 the question was presented:

How does the (inter)national legal framework on human rights provide for governments to limit privacy? What principles govern the exceptions to privacy in this respect?

Within the (inter)national legal framework on human rights there are ample provisions for governments to limit privacy. The relatively open norms in limitation in Article 8(2) ECHR and other international instruments are 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. These grounds are so open-ended that they give opportunity to a rather broad interpretation of limitation grounds which even can be enhanced by creating open norms in secondary (national) law based upon the limitation principle. The limitation provisions are governed by commonly accepted limitation grounds.

I also discussed the 'soft law' coming from the International Commission of Jurists, who met in Siracusa, Sicily in 1984 and defined a set of Principles to consider the limitation and derogation provisions of the International Covenant on Civil and Political Rights. The participants agreed upon the need for a close examination of the conditions and grounds for permissible limitations and derogations enunciated in the Covenant in order to achieve an effective implementation of the rule of law. As frequently emphasized by the General Assembly of the United Nations, a uniform interpretation of limitations on the rights as provided for by the Covenant is of great importance. This should certainly account for the EU and for the ECHR as well. The main principles - in accordance with the law or 'prescribed by law' and 'necessity in a democratic society' - are balanced with the individual right to privacy but should also be applied in the common interest of privacy. When the principle of privacy is endangered, the protection of privacy could also be seen as a public interest and should therefore also be taken into account in the balancing of the right against the intrusion based on 'public interest' in the sense of national security. This could provide for a range of Privacy Impact Assessment procedures within limitation regulations. It is important to stress that limitation of privacy is considered to be any disruption of the 'normal' legal climate by unexpected circumstances. These circumstances have to be defined as clearly as possible within the national legal framework. The main subset of principles to justify the intrusion on privacy in its execution are concerning the legitimacy of the intrusion and the grounds justifying the

limitation. Does the limitation respond to a pressing public or social need? Does it pursue a legitimate aim? Is the limitation proportionate to that aim and are there no other, less intrusive, ways to reach the purpose? These principles are also applied by the ECtHR and should set a secure demarcation how far a state may go in the limitation of privacy. The quintessence is the following principle:

Any assessment as to the necessity of a limitation shall be made on objective considerations.In applying a limitation, a State shall use no more restrictive means than are required for the achievement of the purpose of the limitation. The burden of justifying a limitation upon a right guaranteed under the Covenant lies with the State.

This means that regulations for limitation of privacy shall be based on clear, accessible and objective considerations and that procedures to contest those decisions should be available. Further a transparent procedure to apply limitations, based on the minimal use, proportionality and subsidiarity principle must be in place. The devil is in the details: make those details clear and transparent, no room for function creep and provide for an independent control mechanism: that burden lies with the state.

This demarcation line should be made clearer by answering the question set out in Chapter 4:

How does the European Court on Human Rights validate, in its case law, exceptions to privacy? On what principles are the decisions based?

The limitation of privacy in the examined case law is mainly based on reasons of preventing crime and protecting national security. Although a general conclusion is difficult to present, due to different circumstances and other relevant aspects, the following observations can be made. Competence by government within a democratic society to limit privacy must be based on the law within a democratic society and should provide for a qualitative acceptable law, i.e. giving safeguards against arbitrariness. The notion of necessity to intrude on privacy should be ruled by fair balancing, taking all interests into account, be it public and private interests. Consequently the Court draws the boundaries when the opportunity of surveillance are too broad and not well defined. Generally defined competences are not acceptable. The referred case of Valenzuela Contreras v. Spain of 1998[681] is exemplary:

'Mere suspicion on the part of the police, which in principle serves as the basis for the court's decision, cannot suffice.'

In this case as well as in *Kruslin, Malone* and other referred cases, the ECtHR decided that, concerning the application of the general principles and concerning case-law interferences of Article 8(2) ECHR, restrictions have to be in accordance with the law, referring not merely to the existence and the accessibility of the law by the persons concerned, but also to the quality of the law. [682] Specifically, the aspect of the use of technologically advanced intrusive

[681] ECtHR 30 July 1998, *Valenzuela Contreras v. Spain* [1998] 28 EHRR 483. Also comparable with the refered article 3 DPA in this chapter.

[682] (ii) The words 'in accordance with the law' require that the impugned measure should have some basis in domestic law. However, that expression does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law. The expression thus implies that there must be a measure of protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 (see the Malone judgement cited above, p. 32, § 67). From that requirement stems the need for the law to be accessible to the person concerned, who must, moreover, be able to foresee its

instruments is an aggravating element to be taken in consideration on the delimiting of the competence of governmental intrusion of privacy.

In general the case law of the ECtHR reflects, as a basis for acceptability, the limitation that:

1. *There must be a specific legal rule or regime which authorises the interference with a legitimate aim. Domestic law (has to) provide(s) for various procedural safeguards designed to ensure that the intrusion is not ordered haphazardly, irregularly or without due and proper consideration. It requires the measure to remain under the permanent supervision of a judge.*[683]
2. *The citizen must have adequate access to the law in question; that means it must be comprehendible and accessible*[684].
3. *The law must be formulated with sufficient precision to enable the citizen to foresee the circumstances in which the law would or might be applied and its consequences.*[685]
4. *The necessity of the limitation in a democratic society has to be confirmed by supporting the legitimate aim as pressing social need of that society.*[686]
5. *The intrusion must be proportional and there must be no other (lesser intrusive) means to reach its purpose (subsidiarity/minimisation).*

But even when these elements are in order, it has to be determined, concerning the specifics of the case, if the measures, although legitimate, are well balanced towards the right of the individual and the importance of privacy as common good.

Case law considers in general, conflicts between the interest of an individual and the state. Concerns about the protection of privacy as a common interest are not taken into consideration.

This aspect received some more attention in the telecommunication area as described in Chapter 5, which asked:

Are electronic based investigations, the use of personal data and other judicial coercive measures in the telecommunication field, in particular interception of communications and retention of telecommunication data, compatible with the fundamental right of data protection and privacy?

In this chapter the question was centred on the qualification of electronic based investigations. In particular the use of personal data and other judicial coercive measures in the telecommunication field were held to the mirror of data protection and privacy concerns. The testing field was the interception of communications and retention of telecommunication data. The scope of possible limitations is answered within the case law of the ECtHR and the ICJ of the EU.

National Courts, the ECtHR and the ECJ have proved in their rulings that the principles of proportionality, transparency, purpose specification and independent control have to be guaranteed in the international legal instruments and national law based here upon. The essence

consequences for him (see the Kruslin judgement cited above p. 20, § 27, and the Kopp judgement, p. 540, § 55).

683 Telegraaf Group and Valenzuela Contreras v. Spain.

684 The Sunday Times v United Kingdom) (1979).

685 Sunday Times and Malone v United Kingdom) (1984).

686 Ibidem.

still is, as stated in the ECHR, the ICCPR and the European Charter, that the substantial meaning of the fundamental right may not be destroyed by unsubstantiated limitation. The more radical the limitation will be, the more specific the competences, means and circumstances of the limitation have to be defined in the law. This specifically applies to the technologically advanced instruments of intrusion within the telecommunication sector. More recently, the ECJ stressed the fact that if these intrusions and limitations of privacy have to be exercised, the circumstances and means to do so have to be unambiguously defined in the law and the control on these actions has to be secured by independent institutions. If not, laws can be set aside or ruled illegitimate.

Chapter 6 discussed anti-terrorist and anti-money laundering regulations. The question was:

Are the measures initiated by international governmental organisations and non-governmental fora to control and counter terrorist and other illegitimate activities and their (financial) support, particularly considering the anti-terrorism acts, and, anti-money laundering regulation and procedures, compatible with the fundamental right of data protection and privacy?

Within the specific anti-terrorism and anti money laundering legal instruments on global and European level the main problems are the lack of harmonisation and specification of key-terminology as well in the differentiation in competences of the executive agencies. Furthermore is is clear that there still is the tendency to create open ended rules. This is exemplary in the last EU directive on terrorism and the Fourth Anti-Money Laundering Directive.

This chapter shows that there is a clear development to extend the application of AML and counterterrorist financing regulations and legal descriptions by 'defining' open norms on basis of 'risk' estimation that will give ample opportunity to take investigative action by investigative authorities as law enforcement authorities and other national investigative services as intelligence agencies. There is a danger of 'competence creep' in criminal investigative activities, facilitated in the national and international legal instruments. Although most of the activities of the investigative authorities and intelligence agencies are legitimised by law, the open-ended provisions and lack of independent supervision are not in line with privacy requirements. The scope and purpose of the legal instruments as in the fourth AML Directive are described in broad terms where a more specified application should be in place.

The ruling of the ECJ in the retention case could be of help for a more privacy orientated evaluation of 'limitation instruments' such as the Fourth AML Directive, the retention legislation and the legislation on Counter Terrorist Measures. This is already recognized by the EP report on the proposal of the Commission, specifically concerning the privacy orientation in a 'risk based construction'.

With the 'field work' amongst FIU's and LEA's during the HEMOLIA project it became clear that the disharmony in competences as well as the inconsistency in the terms and procedures used formed the greatest risks and hindrances to effective investigation and detection of crime and terrorist (financing) actions.

The key to applying intrusive measures by the governmental and judicial agencies is considering how they balance the individual's fundamental right of privacy, on the one hand, and the requirements to protect the other rights and common good on the other hand, as

described in Chapters 5 and 6. Criminal investigations and (legal) measures to protect society sometimes require intrusive measures. Within this balancing act it is important to make clear that an interference corresponds with a pressing social need, and any interference must be proportionate to the legitimate aim pursued, meaning that the limitation of personal privacy is 'relevant and sufficient.'

To answer the question of whether the existing regulatory framework suffices and whether adaptations are needed, a general conclusion can be drawn from the case law of the ECtHR and the ECJ and the analysis of the legal framework that provides for the limitations of privacy. The case law elaborates in detail on the principles that should govern the limitation of the fundamental rights of the civilians or 'data subjects'. In addition to these court rulings this thesis aims to reflect and maybe revive the Siracusa Principles as applicable ruler of measurement.[687] A specific reference to these principles is not made in the reasoning of courts as such, the supporting white papers of lawmakers, advice of other international committees such as the WP 29 or in the writings of legal scholars. Although these principles have been defined by a group of well-known international lawyers of an important committee of the United Nations, the relevance seems not to be literarily recognized by the international legal community. Although in essence we find back all principles in the different rulings. Nevertheless, these principles seem not to be elaborated to a sufficiently detailed and clearly specified effect.

The final conclusion of the research question can be that there is a need for dynamics in the boundaries of privacy as well as certain dynamics in the limitation of privacy for the purpose of general interest.[688] The problem is to find the justified balance between those interests where the rights of the individual citizen are taken into account as well as the common good of society, including the general importance of privacy. Therefore a legal framework is required that entails enough transparency as well as clear and harmonised rules for LEAs and NIAs as well as other governmental authorities. At the moment of writing, there is still a deficiency of transparent competences for governmental agencies, be it police, prosecution, FIUs or NIAs. This is made possible by the rather ill-defined and open-ended laws on national levels and the international regulations on EU level as we have seen in existing and future (proposed) privacy regulations and directives, including the Fourth AML Directive.

7.2 First Recommendation

If one thing is clear at the conclusion of this study, it is that scrutiny of the principles for the limitation of privacy should be in place in a more specified and detailed way. The principle of

[687] For reasons of efficiency I have combined the principles when suited. The complete overview is given in the annex III.

[688] In the IRIS project the researchers worde this view as follows: To analyse privacy as a concept for what it is, or should be, the researchers also regard privacy, (at the same time) as a value, a demand and a codified right in relation to security: '*which is broader than the right to data protection, although not separable from it, with special regard to the historical evolution of the concept in which the information element has become of fundamental importance in today's information society – this is especially true in the relationship between privacy and security.* This leads to the overall conclusion that: '*privacy – similarly to security – is not a static concept, not an ideal state that one should endeavour to reach, but a dynamic concept changing throughout historical evolution and depending on the context, which has basic principles and context-dependent elements alike.'*

proportionality of the measures to limit privacy in the name of protecting national security and for the prevention and prosecution of serious crime, including terrorism, is analysed by the European Court of Justice and should be applied in the way it is intended: specifically and with guarantees on independent control. This certainly accounts for the competences of national security agencies. Those agencies seem to be difficult to control, which is inherent in the nature of 'secrecy' of their activities. As made clear by the divulgences of Edward Snowden, many of their actions are tripping over the fuzzy line of their legal competences.

This also accounts for the principle of legality of the measures, closely connected to the principle of proportionality. As mentioned in the evaluation of the retention directive and the ruling of the ECJ in that case, there has to be a well-balanced motivation supporting the decision. This decision must be based on clear and detailed rules of law concerning the rights of the subject and the rights of the State to intrude on these rights to defend other rights and the system as a whole. A legal rule, interpreted light-heartedly bears no legality.

The essence still is, as stated in the ECHR, the ICCPR and the European Charter, that the substantial meaning of the fundamental right may not be destroyed by unsubstantiated limitation. The more radical the limitation, the more specific the competences, means and circumstances of the limitation have to be defined in the law. In this reasoning an important aspect, mentioned by different scholars as well as by the different courts and expert reports, is the fact that the level of possible intrusion into privacy, has been extended immensely by the development of electronic techniques. This asks for a further specification of reasons, purposes, descriptions of used instruments, differentiation of applied measures and independent control on the retention and use of personal data for the purpose of criminal investigations, anti-terrorism and anti-money laundering activities. A good initiative was taken by the European Commission during the evaluation of the Retention Directive concerning a stricter specification in the light of the proportionality principle.

'With a view to meeting the proportionality principle, and in the light of quantitative and qualitative evidence of the value of retained data in Member States, and trends in communications and technologies and in crime and terrorism, the Commission will further consider applying different periods for different categories of data, for different categories of serious crimes or a combination of the two'.[689]

This reasoning in the evaluation of the Retention Directive (see Chapter 5) was explanatory for the negative ruling of the European Court in applying the principle of legitimacy in relation to the proportionality principle in the applicability of modern digital techniques of using personal data by authorities.

7.3 Second Recommendation: Use of the Siracusa Principles

The Siracusa Principles were developed for the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights[690], but are perfectly suited for the European Convention on Human Rights, and the comparable EU and UN instruments. As stated in Chapter 3, these principles are not specifically directed to the State of emergency by external

[689] Evalution Report of the Retention Directive, idem Chapter 5.
[690] Although, as described in Chapter 3, these provisions concern all non absolute rights of the ICCPR, I just refer to the applicability on privacy.

threats to national and international security, but refer to any disruption of the 'normal' legal climate by unexpected circumstances. Chapter 3 described that the applicability of the principles depends on the determination of the 'disruption by unexpected' (i.e. not normal) circumstances, the specification of a disruption of a 'normal legal climate' and the application of special actions by authorities as a result of a balancing of interests of the individual and the society.

The determination about the normalcy of the situation in a given society is highly dependent on that society's own social and legal dynamics and the norms that emerge from them The application of privacy limitations refer to *normal* criminal law and *normal* intelligence law, because disruption of privacy is allowed under specific circumstances that are part of the 'normal' current society. The question is whether regulations based on terrorist intentions and activities supporting those and other criminal activities can be considered normal circumstances in a democratic society. Can those regulations be considered as derogations from the normal legal framework that should always respect fundamental rights?

The non-enumerative specification of general limitation clauses in Article 8(2) ECHR, on one side, and ample competence in the un-harmonised legal framework on ATF and AML among national states on the other side, is heavily disturbing a plausible use of the Siracusa principles on existing and new legal frameworks. Moreover, there are uncontrollable circumstances vaguely described as 'considerations of national security' that seem to justify all intrusions of the personal life of citizens and even the citizens of other states.

The Siracusa Principles can be used in addition to the ECJ and the ECtHR case law to define the boundaries of limitation of privacy that a national authority is allowed to apply.

7.4 The Proof of the Pudding

The legitimacy of a limitation is amongst others based on the specificity of the description and related measures in national or international legal instruments. As posed in Chapter 3: could one say that derogation from the normal situation in which fundamental rights are respected, as described in legal instruments, is a disruption? Or is this a 'normal' situation under different circumstances or for different purposes? This question is not answered in the legal instruments and seems to be more dependent on the actual political situation.

Neither the future European framework to protect privacy, the proposal for a Regulation on the protection of personal data (General Data Protection Regulation) are contemplating on this difficult aspect. Still they could give ample opportunity to regulate the protection in different legal instruments if it considers issues of national security or criminal investigation or any justice matter.[691] The draft Police and Criminal Justice Data Protection Directive should open the way to specify the limitation of privacy relating to personal data concerning research, investigation and prosecuting in cases of security, public order and prevention of crime. A clear

[691] Article 2 states , under e that this Regulation does not apply 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.

differentiation between suspect and non-suspects must be clearly demarcated. Troublingly, this specification seems to be vanished in the recent texts of the proposal.[692]

A clear and transparent policy based on understandable and consequent clauses should be a 'condition sine qua non' for national investigation services in criminal law as well for national security services and other investigative agencies i.a. concerning the financing of terrorist activities. As recently stated by the ICJ: a non-substantiated tapping of conversations between a lawyer and his client by a NIA without independent conclusion of suspicion of endangering state security is not acceptable.[693]

Limitations to intrusive measures by authorities have to be set. This requires clear legislation based upon 'minimal use', proportionality, descriptions of the 'special circumstances' and a credible and independent control mechanism.

It is essential to control the use of the limitation principles. For instance 'the prevention of crime', even 'serious crime', is so inherently system-dependent and non-enumerative that it is often used to refer to a large set of criminal behaviour to use privacy intrusive techniques. The applicability of the principles should not only refer to limitations under obvious 'special circumstances' but also to the 'specific' level of a threat to the democratic society and/or the legal system in a more objective sense. There should be a balanced and proportional decision by a trustworthy authority to avoid endangering the democratic society. The use of certain (legal) instruments to limit privacy or use specific personal data to diminish threats should be clearly described within the national legal instruments.

The object and purposes may never jeopardize the essence of the right concerned as is also accentuated in the Siracusa principles. All limitations of the fundamental rights have to be provided for in the law and should be compatible with the democratic rules in society. Since privacy is a non-absolute right, it has to be protected even more in the sense that its limitation has to be indulged with all possible guarantees against misuse by governmental authorities or third parties. The fact that this non-absolute right can be limited by law also means that those limitations have to be controlled every time a decision is made to limit privacy in a certain way by a certain authority. The control though, is only possible if there is an independent entity that provides for the supervision of the just provisions and application. This is going beyond accidental control mechanisms as for example the Commission for the supervision on the intelligence and security Agencies in The Netherlands. In day to day use of the possibilities to limit the right, by retention laws or by criminal investigation for AML, this control by a judge of instruction for the interception, retention or other use of intrusive technology of tapping is not always the most effective possibility of control.

Therefore a control mechanism has to be developed, including a special cooperation between the privacy supervisory authority and the authority using the limitation possibilities. Until now, the role of the privacy regulator is based upon the privacy laws, therefore excluding regulations concerning prevention or investigating crime and national security issues. This could be

---

[692] *The evolution of law enforcement techniques and methods in the past decade clearly demonstrate that all these categories which fall under the broad category of 'non-suspects' need specific protection. This is especially the case when the processing is not done in a specific criminal investigation or prosecution. It is the difference between information that the law enforcement authorities 'need to know' and the information that is 'nice to have'. Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive00379/13/EN WP 2001.*

[693] ECLI:NL:RBDHA:2015:7436.

changed into a cooperative procedure, possibly with involvement of representatives of the national parliaments.

In this process, it is already possible to base measures on the Covenant. It demands to describe the specific circumstances and preconditions under which a derogation of the agreed civil and political rights are possible. Principles should indicate the conditions under which the authorities (in general) may set aside fundamental rights and under which circumstances. The (general) principles of the limitation clauses can be used to evaluate the limitations in the analysed regulations on privacy, telecommunication, retention and anti-terrorism and AML and ATF rules.

7.5 The Problem of 'Arbitrariness': No limitation Shall be Applied in an Arbitrary and Non-Discriminatory Manner

Every limitation imposed shall be subject to the possibility of challenge to and remedy against its abusive application. This principle can be translated to the principle of 'arbitrariness' ('willekeur') or worst case to abuse of power, 'detournement de pouvoir'. As described in section 4.4.4, arbitrariness can refer to the aspect of Article 8 ECHR to limit this fundamental right 'in accordance with the law or prescribed by law'. The ECtHR ruled that there has to be some basis in domestic law, but it also depends on the quality of the law, meaning that it has to be accessible to the person concerned and foreseeable as to its effects. The law must also indicate the scope of any such discretion conferred on the competent authorities and its exercise must be clear with regard to the legitimate aim of the measures as to sufficient and adequate protection of the subject against arbitrary interference.[694]

The Court made clear that investigations by the secret services have a risk of potentially harming the democratic values of society and therefore require a clear supervision of an impartial supervisory body, as also stated above.[695] This is comparable with the existing and proposed regulations to extend (data) surveillance techniques to encounter (cyber)crime. Independent supervision is necessary for the use of data from electronic communication (retention) and data for AML and ATF as far as they are missing clear limitations on the use

[694] See *Weber and Saravia*, cited above, §§ 93-95 and 145; ECtHR 6 September 2006, *Segerstedt-Wiberg and Others v. Sweden* [2006], App. no. 62332/00, § 76; ECHR 1 October 2008, *Liberty and Others v. the United Kingdom* [2008], App. no. 58243/00, § 62-63; ECHR 18 May 2010, *Kennedy v. the United Kingdom* [2010], App. no. 26839/05, § 152, § 90.

[695] The Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8, that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see *Klass and Others v. Germany*, 6 September 1978, § 56, Series A no. 28, and *Kennedy*, cited above, § 167). However, in both cases the Court was prepared to accept as adequate the independent supervision available. In *Klass and Others*, this included a practice of seeking prior consent to surveillance measures of the G 10 Commission, an independent body chaired by a president who was qualified to hold judicial office and which moreover had the power to order the immediate termination of the measures in question (mutatis mutandis, *Klass and Others*, §§ 21 and 51; see also *Weber and Saravia*, §§ 25 and 117). In *Kennedy* (Ibid) the Court was impressed by the interplay between the Investigatory Powers Tribunal ('IPT'), an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, and the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office (*Kennedy*, § 57) and who had access to all interception warrants and applications for interception warrants (*Kennedy*, § 56), para.100.

of data and the means to use them in the regulations themselves.[696] The righteous use of competence is enhanced by the European Court of Justice ruling on the illegality of the retention directive of 8 April 2014. It is questionable, though, how serious this will be applied in the different national policies concerning future retention regulations.

Coming to the essence of the justifiable limitation, viz. the requirement to do so in whatever is deemed necessary to protect the interests that are mentioned in Article 8(2) of the ECHR, it must be explained how the scales are weighed. One could say that the right of personal freedom is necessary as a guarantee to support society in the functioning of those rights that have been mandated by the individuals to their governments. But, as Scholten reminded us in 1935, although fundamental legal principles may seem undisputed, they find their limitation in other legal principles. The legal principle at stake here is that government is regulating society in order to protect the other 'rights bearers' in protecting the security of society as a whole. This obligation of government and rights of its citizens is often considered to have a higher importance than the individual privacy. What often misses in the considerations of government and even the Courts, is that the general value of protecting privacy is also a common good that has to lay some weight in the scales of decision-making.

As discussed in Chapters 1 and 3, this results in the negative right to privacy, namely the necessity to limit this freedom and thus intrude upon the right to privacy. This possibility is well-accepted in the democratic and certainly in the less democratic societies. The differentiation between those two should lie in the boundaries to the limitations. Limiting the right of privacy in democratic societies has to be justified on the basis of the legitimate aim, the purpose, the proportionality and the fact that there is no other (lesser) means to accomplish that aim (subsidiarity or minimisation principle). Further it has to be acceptable within the opinion of that democratic society within a certain political and cultural structure.

In short, it is the complete interpretation of the contextual interrelationship, practical concordance or 'Ordnungszusammenhang'[697] in balancing (individual) fundamental rights and community interests.

A simple formula of the Siracusa Principles is given to prescribe the use of regulatory instruments to acquire a balance within this concordant system of society, already used in the limitation principles in national and international regulations and specified by the ECtHR and European Court of Justice.

The essence of the requirements to limit the human rights and specifically privacy, lies in the specification of the grounds that are used for the restrictive measures. It is one thing to mention these grounds; it is something else to apply these principles in the decision to limit the fundamental rights on these grounds. The justification lies in the acceptance by the democratic society itself, in the appliance by the authorities, the legal enforcement and the court decisions and possible other (independent) control mechanisms. The already mentioned decision in the Klass case makes it very clear:

---

[696] This of course, will not withhold the EU Commission to stress the importance of personal data-and privacy protection in general terms as provided for in the Fourth AML Directive: *(recital 46) This Directive respects the fundamental rights and observes the principles recognized by the Charter of Fundamental Rights of the European Union, in particular, the respect for private and family life, the right to protection of personal data (…)*

[697] Hesse 1999. (Heidelberg: C.F. Müller, 1995) cited and translated by Thilo Marauhn and Nadine Ruppel, Balancing conflicting Human Rights: Konrad Hesse's notion of 'Praktische Konkordanz' and the German Federal Constitutional Court, in Eva Brems, p. 273 et seq. see paragraph 1.3.1.

(Art. 8-2). 'This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. 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'.[698]

With regards to AML, the fact that terrorist activities can be financed gives reason to limit privacy by processing personal data. Next to that acceptable ground of limitation it is also mentioned that the disturbance of the financial system is reason for far-reaching applications of coercive instruments to fight AML.

'The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes'.

This could endanger the economic system of a democratic society, regarding the existence of a financial crises. It is imaginable that the fact that this will jeopardize the functioning of the European internal market will be enough reason to apply the limitations on data protection and private life.[699] The Siracusa Principles could result in a more limited explanation of the directive. The aspect of proportionality in the legally justified application of privacy limiting measures will be the difficult task for the judicial system. It is to be expected that the ultimate reasoning will be found at the highest Court in last instance, such as the European Court for Human Rights or the European Court of Justice. National courts can lead the way to just interpretations of the leading principles of a democratic society in requests to preliminary questions or if Parties forward their case to ECJ or ECtHR.

A key decision is a ruling of The Netherlands Court of The Hague in a case of *'distressed citizens against the State of The Netherlands'* concerning the international cooperation in the access to and exchange of telecommunication data by intelligence agencies.[700] The Court ruled that the margin of appreciation by the governmental agencies would take into account the guaranties of purpose orientation and proportionality. The use and exchange of 'raw telecommunication data 'concerned a low level of privacy protection. Therefore Article 8 of the ECHR was not endangered by the (unfettered) exchange of telecommunication traffic data between the AIVD and the NSA.

The fact that the exchange of information between national security agencies is a matter of national security justifies the exchange without any further explanation or need to inform the parliament of the origins of the information, according to the Court. This seems a clear example for a preliminary question to the ECtHR.

7.6 Final Observations

One could finish the concluding remarks about the underlying study with the observation that it was a losing game for privacy to begin with. In all cited human rights treaties, as well in the European data protection legal framework it is made clear that privacy is not an absolute right

[698] *Klass* para 42.
[699] Considerations 2, 4, 43, 44 and 49 of the Fourth AML Directive.
[700] The Hague Court, 23-07-2014, ECLI:NL:RBDHA:2014:8966.

and that there are several circumstances that give the authorities the opportunity to limit this fundamental right. This also accounts for the separated fundamental right, or in my view derivative right of privacy, that of personal data protection. But the fact that privacy is not an absolute but dynamic fundamental right requires a non-absolute and dynamic solution where an attentive citizen has to play his role in conscious self-determinations of the values he holds on privacy. Likewise, there is a serious responsibility for the government to set clear rules and develop transparent policies.

In all specific regulations on the use of personal data and the intrusion of the personal sphere of man, be it in criminal law, telecommunication retention law or AML and ATF law, let alone national security law, it is possible to limit the fundamental right on privacy and the protection of personal data and information. And even if these laws and regulations refer to general principles and treaties to respect these fundamental rights, in the same legal instrument it is stated that this protection will not apply in achieving the purpose of the underlying law or treaty if it is a matter of national security or other strategic national interest. The fact that this fundamental right is not absolute should require even more guarantees and controls than absolute fundamental rights because derogation is made possible. This requires a much more specified balancing process and an independent supervisor.

Leading in this process should be the proportionality test. According to the settled case-law of the ECtHR and the ECJ, an act of a state authority as well as the European Union may be regarded as proportionate when the measures which it implements are appropriate for attaining the objectives pursued and do not go beyond what is necessary to achieve those objectives. The Siracusa Principles provide a more transparent balancing process, but the question that remains concerns whether this would fundamentally strengthen the soft body of privacy as a fundamental right. Queer, quoting Helen Nissenbaum, in section 3.5.6 noted that it is questionable if there really are strict limits on incursions into the private lives of citizens.[701]

Those limitations are not strict enough. There always will be an uncontrollable competence of policy concerning national security and other strategic interests of the state within the institutional framework that makes the essence of privacy rather illusory. This aspect is even strengthened by the existing dichotomy between the interests of authorities in their role of privacy regulators and legal enforcement agencies.

Specifically in countries with a strong and impenetrable 'democratic' state system, the risk of almost unavoidable function and competence creep is vast. A clear example is the Zakharov case of 4 December 2015, where Mr. Zakharov, i.a. president of the St Petersburg branch of the Glasnost Defence Foundation, an NGO monitoring the state of media freedom in the Russian regions, which promotes the independence of the regional mass media, freedom of speech and respect for journalists' rights, and provides legal support, including through litigation, to journalists was constantly surveyed because the secret service, the FSB had unlimited access to all telecommunication information, including his-and all other Russian citizens- mobile services. Although he could not present hard proof, the fact that the police and secret service had direct access, without court order and without independent control and remedies was enough for the Court to rule 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

[701] H. Nissenbaum, *Privacy in context*, Stanford Law Books 2010, p. 92.

technical means, to all mobile telephone communications. 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 to destroy the data.[702]

It also has to be taken into account that the processing of all kind of personal data finds place on a global scale. Even if there are specific rules in Europe this will not give guarantees for the rest of the world. As was the case in the ruling of the ECJ in the 'Schrems case' where the 'Safe Harbour' rules were ruled invalid for 'Facebook' because they could not give enough guarantee for the protection of personal data in case they would be processed under the jurisdiction of the USA by the NSA on basis of the 'Patriot' Act.[703]

To make a last remark on the possibility of controlling the limitation of privacy by national authorities, I refer to an interesting fact that can be considered as an integration of Siracusa-like principles in decision making on data protection issues and the possible limitation. The European data protection authorities in their opinion on purpose limitation stipulate that in particular the following key factors need to be taken into account:

1. the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
2. the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
3. the nature of the personal data and the impact of the further processing on the data subjects;
4. the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects. [704]

Processing of personal data in a way that is incompatible with the purposes specified for the collection is against the law and therefore prohibited. A data controller can therefore not legitimise incompatible data processing by simply relying on a new legal ground, such as, for example, in the context of a new security policy or another governmental task.

The purpose limitation principle can only be restricted subject to the conditions set forth in Article 13 of the Privacy Directive. It is unclear why this line of reasoning would not be applicable to the limitation of privacy rights in cases of preventing crimes as terrorist activities and money laundering.

The ultimate consideration though, is the fact that the specified privacy regulations are often ruled out. The application of the essentials of data protection and the protection of personal life is therefore 'hollowed out'. An artificial state of exception, based on the fact that our whole society is under a state of siege by cybercriminals and terrorists, has arguably been created. This is legitimized by the notion that the only purpose of cybercriminals and terrorists is the destruction of our democratic society or the detraction of money and goods in such a way that this is undermining society as well. The only remedy considered to counter this development is the creation of a control mechanism by the government for the issues analysed in this thesis.

[702] ECtHR 4 December 2015, ROMAN ZAKHAROV v. RUSSIA (Application no. 47143/06), par. 302.
[703] Safe Harbour decision (ECJ) of 6 October 2015 Maximilian Schrems v Data Protection Commissioner case (C-362- 14).
[704] WP 29: Opinion March 2013 on purpose limitation.

This control mechanism often lacks an independent entity to control extending powers to investigate social communication, electronic services and financial services.

The legal enforcement agencies' only weapons seem to be found in the increase of investigative powers, using the abundance of information about the citizens of our democratic societies, sometimes based on legal grounds and sometimes based on the fact that it is technologically possible and that it is better to be safe than sorry. I conclude this thesis with some words stated by David Lyon in the introduction of his book about surveillance after September 11:

'In the War on Terrorism the net of suspicion is being cast far and wide and no one, however remote from terrorism, can safely imagine that they are exempt from scrutiny. The loss of some liberties is portrayed as the price for security which is another dubious deal. While tracking down the perpetrators of violence is entirely appropriate and laudable reinforcing surveillance without clear and democratically defined limits is not'.[705]

This reconsideration of the essence of privacy and the limits on its intrusion by a credible legal framework is, under the pressure of the circumstances, more or less repeated by the Obama administration in the last report on big data and the use thereof:

'A legal framework for the protection of privacy interests has grown up in the United States that includes constitutional, federal, State, and common law elements. 'Privacy' is thus not a narrow concept, but instead addresses a range of concerns reflecting different types of intrusion into a person's sense of self, each requiring different protections.'[706]

Given the wide-ranging and deeply intrusive possibilities granted in the inquisitive techniques used by national intelligence agencies and criminals of this world, there must always be some democratically institutionalized system of legitimate rules to control the (secret) controllers even if we know that the soft belly of the privacy rights will be sacrificed without too much hesitation for the values of national security, the prevention of crime and economic prosperity.[707]

If there is an acceptable solution, it has to be found in a dynamic system of privacy controls that will keep pace with changes in society and technological developments with a keen eye on the fundamental integrity of the personal life of citizens all over the world.

[705] D. Lyon, *Surveillance after September 11*, Oxford: Blackwell Publishing Ltd 2003, p. 1.
[706] Big data: seizing opportunities, preserving values, 1 May 2014, <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.
[707] And: Since the 9/11 attacks and the 'war on terror', have human rights become a luxury that we can no longer afford, or must rights always remain a fundamental part of democratic politics since they define the boundary between individual freedom and government tyranny? R.A. Wilson, *Human Rights in the 'War on Terror',* Cambridge University Press 2005.

Summary

The essence of this thesis is the dynamic character of privacy as dependent on place, time, culture and political climate and the need to mold this right to the needs of the common good of society. This process is a never-ending story already known in the Greek city states and probably even before that time.

Privacy, the protection of the personal sphere and personal data in particular, by non-intervention by the government, is a fundamental right for citizens but not an absolute right. Historically the citizens of a society decided theoretically to transfer a part of their individual rights to an authority for the general interest of society.

Although many legal philosophers such as Hobbes, Locke, Rousseau, and even a prominent privacy thinker, Westin, all accept that the exercise of rights of citizens can be transferred in the public interest, there should always be a personal right to (informational) self-determination. Some states, such as the German Federal Republic, are very clear about this by stating this right as such in their constitution. But even Germany accepts that there are circumstances that intrusion into the right to privacy is necessary to secure their democratic society.

This means that the government may curtail this right if the circumstances so require. This is notably the case when there is a threat to national security or any other threat to our democratic society. These limitation possibilities are enshrined in international treaties like the Universal Declaration of Human Rights, the ICCPR and in particular the second part (paragraph 2) of Article 8 of the European Convention for Human Rights (ECHR). The limitation grounds and policies based upon these limitations are integrated in the Member States' legislation. These limitations and considerations are also reflected in EU law and in the legal systems of several non-European countries such as the US by using the possibilities given in the Patriot Act and comparable legislation. The restrictions are not only found in the legislation on the investigative powers of security and justice, but also in telecommunications law and economic and financial (money laundering) legislation.

My research question was whether it is possible to create such restrictions on the right to privacy in such a way that they remain compatible with principles of a democratic society a democratic order.

Because of the vulnerability of the privacy of citizens, restrictions are to be reigned by a set of objective requirements:

1. they must comply with the law;
2. be necessary for the democratic rule of law;
3. be proportional as to the result to be achieved; and,
4. they must be enacted in accordance with accessible and foreseeable legislative transparency of the rules.

It is important that law that limits privacy does not contain or consists of vague concepts and definitions or unclear competences for legal enforcement agencies and other governmental agencies. The main obstacles, as described in this thesis, to finding a justified result in the

balancing between the individual and general right to privacy and the acceptable intrusion by authorities, are due to the peculiar vagueness of definitions and the dis-harmonisation of regulations amongst the states that have to apply those regulations. This thesis analyses in this context law on anti-terrorism, anti- money laundering to support terrorist activities and data retention rules.

In several rulings of the European Court of Human Rights and the European Court of Justice deal with the (un)lawfulness of the restrictions. The most revolutionary ECJ case in this respect was the annulment of the so called Retention Directive on 8 April 2014, because the legal justification to store telecommunication data of all European citizens lacked legitimation and legal guarantees.

The other legal peculiarity that is described in this thesis is the fact that soft law, without too much hesitation, is transferred into hard law. This is for instance the case in the field of anti-money laundering and terrorist financing by the so called' Financial Task Force, FATF that creates a soft-law framework. These 'informal' deliberations to prevent money laundering and terrorist financing have led to a list of 49 principles which are almost literarily copied into EU legislation as the Fourth Anti-Money Laundering Directive and national law implementing this Directive.

The result is that rather vague concepts as the 'risk based' principle are accepted in international and national law for the investigation and prosecution of money-laundering and anti-terrorism without proper definition or even a description of its meaning.

These concepts are the result of the fact that advanced technological developments result in more intrusive techniques, available for governmental agencies in enforcement as well available to terrorists and other criminals. The activities of the aforementioned parties are used by legal enforcement agencies to justify the use of further intrusive techniques and policies to perform their tasks to prevent the risk of undermining our democratic societies.

What I have found in my research is that privacy and protection of personal data are subject to the dynamics of the political situation, as well as the availability of new intrusive technologies. It shows a wave cycle: After a wave of new rules to increase the competencies for intelligence and law enforcement after 9/11, we see a softening and critical notion on those activities after the revelations of Snowden and the disclosures of intelligence agencies spying on each other and on their own and foreign citizens and politicians with the help of information-technology. Lately, there is again a reinforcement of surveillance and interception powers after the terrorist attacks in Paris and Brussels. Surveillance acts in the UK, France and The Netherlands are criticized but have passed through parliament without too much trouble. The citizens themselves should be more involved in the magnitude of the transfer of their privacy rights and whether the government is intruding on their privacy in a proper and justified way. This should be done by a more active and controlling role of the parliament and an independent control authority with regard to the implementation of the mitigation measures.

This conclusion regarding independence and clarity of scope of responsibilities and definitions, is drawn by both the European Court of Justice regarding the unlimited storage and use of telecommunications data of citizens, as well as by the European Court of Human Rights in respect of the use of advanced interception and surveillance techniques.
There should be no choice between the justification of the right to protection of national security against terrorism on the one hand and privacy on the other hand. The government has

a duty and responsibility to ensure both ‘rights’ through the implementation of rules and policies. If a government does not abide by this principle, or is willfully acting contrary to the demands of a democratic order by restricting fundamental rights, there is no legitimization of its existence. In an important ruling of the ECtHR, the Court states that the restrictive measure on a fundamental right to secure democratic society may never have the impact that the fundamental right disappears and consequently the democratic system that is based on those fundamental rights. It is therefore of utmost importance that an independent balancing of interests mechanism consists in the introduction and implementation of privacy restrictions which is taking into account all the interests of a democratic order.

As concluded in this thesis the leading principle in this balancing process should be the proportionality test. According to the settled case-law of the ECtHR and the ECJ, an act of a state authority as well as the European Union may be regarded as proportionate when the measures which it implements are appropriate for attaining the objectives pursued and do not go beyond what is necessary to achieve those objectives. Additionally,the so called Siracusa Principles that I discuss in this thesis, provide a more transparent balancing process. Looking out to a ‘geo-logical’ landscape of increasing information, communication and robotic technology, and the perceived existence of uncontrollable terrorist threats, creates the attraction for law enforcement and intelligence agencies to use these techniques on a wide scale to pursue ‘persons of interest’.

When limitations on privacy are not defined specifically in law and the use of intrusive competencies and techniques are not strictly demarcated, the proportionality principle and the balancing process will be hollow instruments. There always will be an uncontrollable competence of policy concerning national security and other strategic interests of the state within the institutional framework. This aspect is even strengthened by the existing dichotomy between the interests of authorities in their role of privacy regulators and legal enforcement agencies.

The difficult tasks of governments in this vulnerable information age is to find a credible solution to balance the individual privacy as well as the common principle to protect such fundamental rights to deserve the notion of democratic society with other common principles such as creating a safe society for citizens.

If there is an acceptable solution, it has to be found in a dynamic system of privacy controls that will keep pace with changes in society and technological developments with a keen eye on the fundamental integrity of the personal life of citizens all over the world.

Annex I FATF

Members FATF:

(the globe.)

Argentina	Finland	Ireland	Russian Federation
Australia	France	Italy	Singapore
Austria	Germany	Japan	South Africa
Belgium	Greece	Republic of Korea	Spain
Brazil	*Gulf Co-operation Council*	Luxembourg	Sweden
Canada	Hong Kong, China	Mexico	Switzerland
China	Iceland	The Netherlands, Kingdom of	Turkey
Denmark	India	New Zealand	United Kingdom
European Commission		Norway	United States
		Portugal	

FATF Associate Members

- Asia/Pacific Group on Money Laundering (APG) *(See also: APG website)*
- Caribbean Financial Action Task Force (CFATF) *(See also: CFATF website)*
- Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) *(See also: Moneyval website)*
- Eurasian Group (EAG) *(See also: EAG website)*
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *(See also: ESAAMLG website)*
- Financial Action Task Force on Money Laundering in South America (GAFISUD) *(See also: GAFISUD Website)*
- Inter Governmental Action Group against Money Laundering in West Africa (GIABA) *(See also: GIABA website)*
- Middle East and North Africa Financial Action Task Force (MENAFATF) *(See also: MENAFATF website)*

FATF Observers

The following international organisations have observer status with the FATF. The international organisations listed are those which have, among other functions, a specific anti-money laundering mission or function. To access additional information on any of these bodies or organisations, select the appropriate hyperlink.

- African Development Bank
- Anti-Money Laundering Liaison Committee of the Franc Zone (CLAB), [for more information, see the website of the Banque de France]
- Asian Development Bank
- Basel Committee on Banking Supervision (BCBS)
- Commonwealth Secretariat
- Egmont Group of Financial Intelligence Units
- European Bank for Reconstruction and Development (EBRD)
  See Additional information
- European Central Bank (ECB)
  See Additional information
- Eurojust
- Europol
- Group of International Finance Centre Supervisors (GIFCS) *[formerly the Offshore Group of Banking Supervisors - OGBS]*
- Inter-American Development Bank (IDB)
- International Association of Insurance Supervisors (IAIS)
- International Monetary Fund (IMF)
  See Additional information
- International Organisation of Securities Commissions (IOSCO)

- Interpol
  Interpol/Money Laundering*[English]*
  See Additional information
- Organization of American States / Inter-American Committee Against Terrorism (OAS/CICTE)
- Organization of American States / Inter-American Drug Abuse Control Commission (OAS/CICAD)
  See Additional information
- Organisation for Economic Co-operation and Development (OECD)
  See Additional information
- Task Force on Money Laundering in Central Africa (GABAC)
- United Nations -
- Office on Drugs and Crime (UNODC)
  See Additional information
  Counter-Terrorism Committee of the Security Council (UNCTC)
  See Additional information
- The Al-Qaida and Taliban Sanctions Committee (1267 Committee)
- World Bank
- World Customs Organization (WCO)

Annex II FATF recommendations

FATF Recommendations 2012

A – AML/CFT POLICIES AND COORDINATION

1 - Assessing risks & applying a risk-based approach
2 - National cooperation and coordination

B – MONEY LAUNDERING AND CONFISCATION

3 - Money laundering offence
4 - Confiscation and provisional measures

C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5 - SRII Terrorist financing offence
6 - SRIII Targeted financial sanctions related to terrorism & terrorist financing
7 - Targeted financial sanctions related to proliferation
8 - Non-profit organisations

D – PREVENTIVE MEASURES

9 - Financial institution secrecy laws

Customer due diligence and record keeping

10 - Customer due diligence
11 - Record keeping

Additional measures for specific customers and activities

12 - Politically exposed persons
13 - Correspondent banking
14 - Money or value transfer services
15 - New technologies
16 - Wire transfers

Reliance, Controls and Financial Groups

17 - Reliance on third parties
18 - Internal controls and foreign branches and subsidiaries
19 - Higher-risk countries

Reporting of suspicious transactions

20 - Reporting of suspicious transactions
21 - Tipping-off and confidentiality

Designated non-financial Businesses and Professions (DNFBPs)

22 - DNFBPs: Customer due diligence
23 - DNFBPs: Other measures

E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24 - Transparency and beneficial ownership of legal persons
25 - Transparency and beneficial ownership of legal arrangements

F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES

Regulation and Supervision

26 - Regulation and supervision of financial institutions
27 - Powers of supervisors
28 - Regulation and supervision of DNFBPs

Operational and Law Enforcement

29 - Financial intelligence units
30 - Responsibilities of law enforcement and investigative authorities
31 - Powers of law enforcement and investigative authorities
32 - Cash couriers

General Requirements

33 - Statistics
34 - Guidance and feedback

Sanctions

35 - Sanctions

G – INTERNATIONAL COOPERATION

36 - International instruments
37 - Mutual legal assistance
38 - Mutual legal assistance: freezing and confiscation
39 - Extradition
40 - Other forms of international cooperation

Annex III Siracusa Principles

United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities, Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984).

I. Limitation Clauses

A. General Interpretative Principles Relating to the Justification of Limitations

B. Interpretative Principles Relating to Specific Limitation Clauses

i. 'prescribed by law'

ii. 'in a democratic society'

iii. 'public order (ordre public)'

iv. 'public health'

v. 'public morals'

vi. 'national security'

vii. 'public safety'

viii. 'rights and freedoms of others,' or 'rights and reputations of others'

ix. 'restrictions on public trial'

II. Derogations in a Public Emergency

A. 'Public Emergency Which Threatens the Life of the Nation'

B. Proclamation, Notification, and Termination of a Public Emergency

C. 'Strictly Required by the Exigencies of the Situation'

D. Non-Derogable Rights

E. Some General Principles on the Introduction and Application of a Public Emergency and Consequent Derogation Measures

F. Recommendations Concerning the Functions and Duties of the Human Rights Committee and United Nations Bodies

I. LIMITATION CLAUSES

A. General Interpretative Principles Relating to the Justification of Limitations*

1. No limitations or grounds for applying them to rights guaranteed by the Covenant are permitted other than those contained in the terms of the Covenant itself.
2. The scope of a limitation referred to in the Covenant shall not be interpreted so as to jeopardize the essence of the right concerned.
3. All limitation clauses shall be interpreted strictly and in favour of the rights at issue.
4. All limitations shall be interpreted in the light and context of the particular right concerned.
5. All limitations on a right recognized by the Covenant shall be provided for by law and be compatible with the objects and purposes of the Covenant.
6. No limitation referred to in the Covenant shall be applied for any purpose other than that for which it has been prescribed.
7. No limitation shall be applied in an arbitrary manner.
8. Every limitation imposed shall be subject to the possibility of challenge to and remedy against its abusive application.
9. No limitation on a right recognized by the Covenant shall discriminate contrary to Article 2, paragraph 1.
10. Whenever a limitation is required in the terms of the Covenant to be 'necessary,' this term implies that the limitation:
    (a) is based on one of the grounds justifying limitations recognized by the relevant Article of the Covenant,
    (b) responds to a pressing public or social need,
    (c) pursues a legitimate aim, and
    (d) is proportionate to that aim.

    Any assessment as to the necessity of a limitation shall be made on objective considerations.
11. In applying a limitation, a State shall use no more restrictive means than are required for the achievement of the purpose of the limitation.
12. The burden of justifying a limitation upon a right guaranteed under the Covenant lies with the State.
13. The requirement expressed in Article 12 of the Covenant, that any restrictions be consistent with other rights recognized in the Covenant, is implicit in limitations to the other rights recognized in the Covenant.
14. The limitation clauses of the Covenant shall not be interpreted to restrict the exercise of any human rights protected to a greater extent by other international obligations binding upon the State.

B. Interpretative Principles Relating to Specific Limitation Clauses

i. 'prescribed by law'

15. No limitation on the exercise of human rights shall be made unless provided for by national law of general application which is consistent with the Covenant and is in force at the time the limitation is applied.

16. Laws imposing limitations on the exercise of human rights shall not be arbitrary or unreasonable.

17. Legal rules limiting the exercise of human rights shall be clear and accessible to everyone.

18. Adequate safeguards and effective remedies shall be provided by law against illegal or abusive imposition or application of limitations on human rights.

ii. 'in a democratic society'

19. The expression 'in a democratic society' shall be interpreted as imposing a further restriction on the limitation clauses it qualifies.

20. The burden is upon a State imposing limitations so qualified to demonstrate that the limitations do not impair the democratic functioning of the society.

21. While there is no single model of a democratic society, a society which recognizes and respects the human rights set forth in the United Nations Charter and the Universal Declaration of Human Rights may be viewed as meeting this definition.

iii. 'public order (ordre public)'

22. The expression 'public order (ordre public)' as used in the Covenant may be defined as the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded. Respect for human rights is part of public order (ordre public).

23. Public order (ordre public) shall be interpreted in the context of the purpose of the particular human right which is limited on this ground.

24. State organs or agents responsible for the maintenance of public order (ordre public) shall be subject to controls in the exercise of their power through the parliament, courts, or other competent independent bodies.

iv. 'public health'

25. Public health may be invoked as a ground for limiting certain rights in order to allow a State to take measures dealing with a serious threat to the health of the population or individual members of the population. These measures must be specifically aimed at preventing disease or injury or providing care for the sick and injured.

26. Due regard shall be had to the international health regulations of the World Health Organization.

v. 'public morals'

27. Since public morality varies over time and from one culture to another, a State which invokes public morality as a ground for restricting human rights, while enjoying a certain margin of discretion, shall demonstrate that the limitation in question is essential to the maintenance of respect for fundamental values of the community.

28. The margin of discretion left to states does not apply to the rule of non-discrimination as defined in the Covenant.

vi. 'national security'

29. National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.

30. National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.

31. National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.

32. The systematic violation of human rights undermines true national security and may jeopardize international peace and security. A State responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population.

vii. 'public safety'

33. Public safety means protection against danger to the safety of persons, to their life or physical integrity, or serious damage to their property.

34. The need to protect public safety can justify limitations provided by law. It cannot be used for imposing vague or arbitrary limitations and may only be invoked when there exist adequate safeguards and effective remedies against abuse.

viii. 'rights and freedoms of others' or the 'rights or reputations of others'

35. The scope of the rights and freedoms of others that may act as a limitation upon rights in the Covenant extends beyond the rights and freedoms recognized in the Covenant.

36. When a conflict exists between a right protected in the Covenant and one which is not, recognition and consideration should be given to the fact that the Covenant seeks to protect the most fundamental rights and freedoms. In this context especial weight should be afforded to rights not subject to limitations in the Covenant.

37. A limitation to a human right based upon the reputation of others shall not be used to protect the State and its officials from public opinion or criticism.

ix. 'restrictions on public trial'

38. All trials shall be public unless the Court determines in accordance with law that:

(a) the press or the public should be excluded from all or part of a trial on the basis of specific findings announced in open court showing that the interest of the private lives of the parties or their families or of juveniles so requires; or

(b) the exclusion is strictly necessary to avoid publicity prejudicial to the fairness of the trial or endangering public morals, public order (ordre public), or national security in a democratic society.

II. DEROGATIONS IN A PUBLIC EMERGENCY

A. 'Public Emergency which Threatens the Life of the Nation'

39. A State party may take measures derogating from its obligations under the International Covenant on Civil and Political Rights pursuant to Article 4 (hereinafter called 'derogation measures') only when faced with a situation of exceptional and actual or imminent danger which threatens the life of the nation. A threat to the life of the nation is one that:

(a) affects the whole of the population and either the whole or part of the territory of the State, and

(b) threatens the physical integrity of the population, the political independence or the territorial integrity of the State or the existence or basic functioning of institutions indispensable to ensure and project the rights recognized in the Covenant.

40. Internal conflict and unrest that do not constitute a grave and imminent threat to the life of the nation cannot justify derogations under Article 4.

41. Economic difficulties per se cannot justify derogation measures.

B. Proclamation, Notification, and Termination of a Public Emergency

42. A State party derogating from its obligations under the Covenant shall make an official proclamation of the existence of the public emergency threatening the life of the nation.

43. Procedures under national law for the proclamation of a State of emergency shall be prescribed in advance of the emergency.

44. A State party derogating from its obligations under the Covenant shall immediately notify the other states parties to the Covenant, through the intermediary of the Secretary-General of the United Nations, of the provisions from which it has derogated and the reasons by which it was actuated.

45. The notification shall contain sufficient information to permit the states parties to exercise their rights and discharge their obligations under the Covenant. In particular it shall contain:

(a) the provisions of the Covenant from which it has derogated;

(b) a copy of the proclamation of emergency, together with the constitutional provisions, legislation, or decrees governing the State of emergency in order to assist the states parties to appreciate the scope of the derogation;

(c) the effective date of the imposition of the State of emergency and the period for which it has been proclaimed;

(d) an explanation of the reasons which actuated the government's decision to derogate, including a brief description of the factual circumstances leading up to the proclamation of the State of emergency; and

(e) a brief description of the anticipated effect of the derogation measures on the rights recognized by the Covenant, including copies of decrees derogating from these rights issued prior to the notification.

46. States parties may require that further information necessary to enable them to carry out their role under the Covenant be provided through the intermediary of the Secretary-General.

47. A State party which fails to make an immediate notification in due form of its derogation is in breach of its obligations to other states parties and may be deprived of the defenses otherwise available to it in procedures under the Covenant.

48. A State party availing itself of the right of derogation pursuant to Article 4 shall terminate such derogation in the shortest time required to bring to an end the public emergency which threatens the life of the nation.

49. The State party shall on the date on which it terminates such derogation inform the other State parties, through the intermediary of the Secretary-General of the United Nations, of the fact of the termination.

50. On the termination of a derogation pursuant to Article 4 all rights and freedoms protected by the Covenant shall be restored in full. A review of the continuing consequences of derogation measures shall be made as soon as possible. Steps shall be taken to correct injustices and to compensate those who have suffered injustice during or in consequence of the derogation measures.

C. 'Strictly Required by the Exigencies of the Situation'

51. The severity, duration, and geographic scope of any derogation measure shall be such only as are strictly necessary to deal with the threat to the life of the nation and are proportionate to its nature and extent.

52. The competent national authorities shall be under a duty to assess individually the necessity of any derogation measure taken or proposed to deal with the specific dangers posed by the emergency.

53. A measure is not strictly required by the exigencies of the situation where ordinary measures permissible under the specific limitations clauses of the Covenant would be adequate to deal with the threat to the life of the nation.

54. The principle of strict necessity shall be applied in an objective manner. Each measure shall be directed to an actual, clear, present, or imminent danger and may not be imposed merely because of an apprehension of potential danger.

55. The national constitution and laws governing states of emergency shall provide for prompt and periodic independent review by the legislature of the necessity for derogation measures.

56. Effective remedies shall be available to persons claiming that derogation measures affecting them are not strictly required by the exigencies of the situation.

57. In determining whether derogation measures are strictly required by the exigencies of the situation the judgment of the national authorities cannot be accepted as conclusive.

D. Non-Derogable Rights

58. No State party shall, even in time of emergency threatening the life of the nation, derogate from the Covenant's guarantees of the right to life; freedom from torture, cruel, inhuman or degrading treatment or punishment, and from medical or scientific experimentation without free consent; freedom from slavery or involuntary servitude; the right not to be imprisoned for contractual debt; the right not to be convicted or sentenced to a heavier penalty by virtue of retroactive criminal legislation; the right to recognition as a person before the law; and freedom of thought, conscience and religion. These rights are not derogable under any conditions even for the asserted purpose of preserving the life of the nation.

59. State parties to the Covenant, as part of their obligation to ensure the enjoyment of these rights to all persons within their jurisdiction (Art. 2(1)) and to adopt measures to secure an effective remedy for violations (Art. 2(3)), shall take special precautions in time of public emergency to ensure that neither official nor semi-official groups engage in a practice of arbitrary and extra-judicial killings or involuntary disappearances, that persons in detention are protected against torture and other forms of cruel, inhuman or degrading treatment or

punishment, and that no persons are convicted or punished under laws or decrees with retroactive effect.

60. The ordinary courts shall maintain their jurisdiction, even in a time of public emergency, to adjudicate any complaint that a non-derogable right has been violated.

E. Some General Principles on the Introduction and Application of a Public Emergency and Consequent Derogation Measures

61. Derogation from rights recognized under international law in order to respond to a threat to the life of the nation is not exercised in a legal vacuum. It is authorized by law and as such it is subject to several legal principles of general application.

62. A proclamation of a public emergency shall be made in good faith based upon an objective assessment of the situation in order to determine to what extent, if any, it poses a threat to the life of the nation. A proclamation of a public emergency, and consequent derogations from Covenant obligations, that are not made in good faith are violations of international law.

63. The provisions of the Covenant allowing for certain derogations in a public emergency are to be interpreted restrictively.

64. In a public emergency the rule of law shall still prevail. Derogation is an authorized and limited prerogative in order to respond adequately to a threat to the life of the nation. The derogating State shall burden of justifying its actions under law.

65. The Covenant subordinates all procedures to the basic objectives of human rights. Article 5(1) of the Covenant sets definite limits to actions taken under the Covenant:

> Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant.

Article 29(2) of the Universal Declaration of Human Rights sets out the ultimate purpose of law:

> In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

These provisions apply with full force to claims that a situation constitutes a threat to the life of a nation and hence enables authorities to derogate.

66. A bona fide proclamation of the public emergency permits derogation from specified obligations in the Covenant, but does not authorize a general departure from international obligations. The Covenant in Article 4(1) and 5(2) expressly prohibits derogations which are inconsistent with other obligations under international law. In this regard, particular note should be taken of international obligations which apply in a public emergency under the Geneva and I.L.O. Conventions.

67. In a situation of a non-international armed conflict a State party to the 1949 Geneva Conventions for the protection of war victims may under no circumstances suspend the right to a trial by a court offering the essential guarantees of independence and impartiality (Article 3 common to the 1949 Conventions). Under the 1977 additional Protocol Ⅱ, the

following rights with respect to penal prosecution shall be respected under all circumstances by State parties to the Protocol:

(a) the duty to give notice of changes without delay and to grant the necessary rights and means of defence;

(b) conviction only on the basis of individual penal responsibility;

(c) the right not to be convicted, or sentenced to a heavier penalty, by virtue of retroactive criminal legislation;

(d) presumption of innocence;

(e) trial in the presence of the accused;

(f) no obligation on the accused to testify against himself or to confess guilt;

(g) the duty to advise the convicted person on judicial and other remedies.

68. The I.L.O. basic human rights conventions contain a number of rights dealing with such matters as forced labour, freedom of association, equality in employment and trade union and workers' rights which are not subject to derogation during an emergency; others permit derogation, but only to the extent strictly necessary to meet the exigencies of the situation.

69. No State, including those that are not parties to the Covenant, may suspend or violate, even in times of public emergency:

(a) the right to life;

(b) freedom from torture or cruel, inhuman or degrading treatment or punishment and from medical or scientific experimentation;

(c) the right not to be held in slavery or involuntary servitude; and,

(d) the right not to be subjected to retroactive criminal penalties as defined in the Covenant.

Customary international law prohibits in all circumstances the denial of such fundamental rights.

70. Although protections against arbitrary arrest and detention (Art. 9) and the right to a fair and public hearing in the determination of a criminal charge (Art. 14) may be subject to legitimate limitations if strictly required by the exigencies of an emergency situation, the denial of certain rights fundamental to human dignity can never be strictly necessary in any conceivable emergency. Respect for these fundamental rights is essential in order to ensure enjoyment of non-derogable rights and to provide an effective remedy against their violation. In particular:

(a) all arrests and detention and the place of detention shall be recorded, if possible centrally, and make available to the public without delay;

(b) no person shall be detained for an indefinite period of time, whether detained pending judicial investigation or trial or detained without charge;

(c) no person shall be held in isolation without communication with his family, friend, or lawyer for longer than a few days, e.g., three to seven days;

(d) where persons are detained without charge the need of their continued detention shall be considered periodically by an independent review tribunal;

(e) any person charged with an offense shall be entitled to a fair trial by a competent, independent and impartial court established by law;

(f) civilians shall normally be tried by the ordinary courts; where it is found strictly necessary to establish military tribunals or special courts to try civilians, their competence, independence and impartiality shall be ensured and the need for them reviewed periodically by the competent authority;

(g) any person charged with a criminal offense shall be entitled to the presumption of innocence and to at least the following rights to ensure a fair trial:

— the right to be informed of the charges promptly, in detail and in a language he understands,

— the right to have adequate time and facilities to prepare the defence including the right to communicate confidentially with his lawyer,

— the right to a lawyer of his choice, with free legal assistance if he does not have the means to pay for it,

— the right to be present at the trial,

— the right not to be compelled to testify against himself or to make a confession,

— the right to obtain the attendance and examination of defence witnesses,

— the right to be tried in public save where the court orders otherwise on grounds of security with adequate safeguards to prevent abuse,

— the right to appeal to a higher court;

(h) an adequate record of the proceedings shall be kept in all cases; and,

(i) no person shall be tried or punished again for an offense for which he has already been convicted or acquitted.

F. Recommendations Concerning the Functions and Duties of the Human Rights Committee and United Nations Bodies

71. In the exercise of its power to study, report, and make general comments on states parties' reports under Article 40 of the Covenant, the Human Rights Committee may and should examine the compliance of states parties with the provisions of Article 4. Likewise it may and should do so when exercising its powers in relevant cases under Article 41 and the Optional Protocol relating, respectively, to interstate and individual communications.

72. In order to determine whether the requirements of Article 4(1) and (2) have been met and for the purpose of supplementing information in states parties' reports, members of the Human Rights Committee, as persons of recognized competence in the field of human rights, may and should have regard to information they consider to be reliable provided by other inter-governmental bodies, non-governmental organizations, and individual communications.

73. The Human Rights Committee should develop a procedure for requesting additional reports under Article 40(1)(b) from states parties which have given notification of derogation under Article 4(3) or which are reasonably believed by the Committee to have imposed emergency measures subject to Article 4 constraints. Such additional reports should relate to questions concerning the emergency insofar as it affects the implementation of the Covenant and should be dealt with by the Committee at the earliest possible date.

74. In order to enable the Human Rights Committee to perform its fact-finding functions more effectively, the committee should develop its procedures for the consideration of communications under the Optional Protocol to permit the hearing of oral submissions and

evidence as well as visits to states parties alleged to be in violation of the Covenant. If necessary, the states parties to the Optional Protocol should consider amending it to this effect.

75. The United Nations Commission on Human Rights should request its Sub-Commission on Prevention of Discrimination and Protection of Minorities to prepare an annual list if states, whether parties to the Covenant or not, that proclaim, maintain, or terminate a public emergency together with:

    (a) in the case of a State party, the proclamation and notification; and,

    (b) in the case of other states, any available and apparently reliable information concerning the proclamation, threat to the life of the nation, derogation measures and their proportionality, non-discrimination, and respect for non-derogable rights.

76. The United Nations Commission on Human Rights and its Sub-Commission should continue to utilize the technique of appointment of special rapporteurs and investigatory and fact-finding bodies in relation to prolonged public emergencies.

[*] The term ‘limitations' in these principles includes the term ‘restrictions’ as used in the Covenant.

Bibliography

Agamben 1995

G. Agamben, 'The Sacred or Accursed Man', in *Homo Sacer: Sovereign Power and Bare Life* (originally published as Homo Sacer. Il potere sovrano e la nuda vita, Giulio Einaudi editore s.p.a. 1995) Stanford, CA: Stanford University Press 1998.

Agamben 2005

G. Agamben, *State of Exception*, University of Chicago Press 2005

Albrecht & Kilchling 2009

H-J. Albrecht & M. Kilchling, 'Die Überwachung von Telekommunikations-Verkehrsdaten'. In: *Jahrbuch 2009 der Max-Planck-Gesellschaft* 2009.

Albrecht, Grafe & Kilchling 2008

H-J. Albrecht, A. Grafe, M. Kilchling, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO*, Berlin: Duncker & Humblot 2008.

Altman 1975

I. Altman, *The environment and Social Behaviour: Privacy, Personal Space, Territory, Crowding*, Monterey, CA: Brooks/Cole 1975.

Arangio-Ruiz 2000

G. Arangio-Ruiz, 'On the Security Council's 'Law-Making'', 83 *Rivista di diritto internazionale* 2000.

Bantekas 2003

I. Bantekas, 'The International Law of Terrorist Financing', *The American Journal of International Law* 2003, Vol. 97, No. 2, pp. 315-333.

Barnidge 2007

R.P. Barnidge, *Non-State Actors and Terrorism: Applying the Law of State Responsibility and the Due Diligence Principle*, The Hague: T.M.C. Asser Instituut and Contributors 2007.

Beck 1992

U. Beck, *Risk Society: Towards a New Modernity*, London: Sage Publications 1992

Bennett 1992

C. Bennett, Regulating Privacy: *Data Protection and Public Policy in Europe and the United States*, New York: Cornell University Press 1992.

Bianchi 2007

A. Bianchi, 'Assessing the Effectiveness of the UN Security Council's Anti-terrorism Measures: The Quest for Legitimacy and Cohesion', *European Journal of International Law* 2007, Vol. 17, No. 5, pp. 881-919.

Bloustein 1964

E.J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York University Law Review* 1964, Vol. 39, No. 6, pp. 1002-07.

Borgers 2012

M.J. Borgers, 'Framework Decision on Combating Terrorism: Two Questions on the Definition of Terrorist Offences', *New Journal of European Criminal Law* 2012, No. 1, pp. 68-82.

Boyer 2004

A.D. Boyer, *Law, liberty, and Parliament: Selected Essays on the Writings of Sir Edward Coke*, Indianapolis: Liberty Fund 2004.

Boyle 1982

F. Boyle, 'The Entebbe Hostage Crisis', *The Netherlands ILR* 1982, Vol. 29, No. 1, p. 32.

Brown 2010

I. Brown, 'Communications Data Retention in an Evolving Internet', *International Journal of Law and Information Technology*, Oxford University Press 2010, Vol. 19 No. 2, pp. 95-109.

Buruma 2005

Y. Buruma, *De dreigingsspiraal. Onbedoelde neveneffect van misdaadbestrijding*, Den Haag: Boom Juridische uitgevers 2005

Calo 2011

Calo M.R., The Bounderies of Privacy Harm, Indiana Law Journal, Vol. 86:1131- 1161

Cameron 2000

I. Cameron, *National Security and the European Convention on Human Rights*, The Hague-London-Boston: Kluwer Law International 2000.

Cheng 2006

B. Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, Cambridge: Cambridge University Press 2006.

Christoffersen 2009

J. Christoffersen, *Fair balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights*, Leiden/Boston: Martinus Nijhoff 2009, .

Clarke 1996

R. Clarke, 'Privacy and Dataveillance, and Organisational Strategy', *Proc. I.S. Audit & Control Association (EDPAC'96)*, Perth 1996.

Conte 2010

A. Conte, *Human Rights in the Prevention and Punishment of Terrorism: Commonwealth Aproaches in the UK, Canada, Australia and New Zealand*, Springer-Verlag Berlin Heidelberg 2010.

Cooley 1888

T. Cooley, *A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Powers of the States of the American Union*, Boston: Little, Brown, and Company 1888, 8th ed. 1927.

Cooley 1888

T.M. Cooley, *A Treatise on the Law of Torts*, Callaghan and Company 1888, 2d ed.

Crump 2003

C. Crump, 'Data Retention:Privacy, Anonymity and Accountability Online', *Stanford Law Review* 2003, Vol. 56, No. 1, pp. 191-230.

Custers 2008

B. Custers, 'Tapping and Data Retention in Ultrafast Communication Networks', *Journal of International Commercial Law and Technology* 2008, Vol. 3, No. 2, pp. 94-100.

Daes 1990

E-I. Daes: *Freedom of the Individual under Law: A Study of the Individual's Duties to the Community and the Limitations on Human Rights and Freedoms under Article 29 of the Universal Declaration of Human Rights*, New York: United Nations. Centre for Human Rights 1990, p. 72 § 40 and p. 74 § 57-62, on p. 80, note 458 and note 461.

Van Dijk & Van Hoof

Theory and Practice of the European Convention on Human Rights, Pieter van Dijk,Godefridus J. H. Hoof,G. J. H. Van Hoof, 1979, 1984, 1998.

Van Est, Dijstelbloem & Van 't Hof 2008

R. van Est, H. Dijstelbloem & C. van 't Hof, *Het Glazen Lichaam: Gegrepen door informatie*, Den Haag: Rathenau Instituut 2008.

Feldman 1994

D. Feldman, 'Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty', *Current Legal Problems* 1994, Vol. 47, No. 2, pp. 41-71.

Fenwick 2002

H. Fenwick , 'The Anti-Terrorism, Crime and Security Act 2001: A Proportionate Response to 11 September?', *The Modern Law Review* 2002, Vol. 65, No. 5, pp.724-762.

Fialová 2012

E. Fialová, *Data Retention: Four Times Unconstitutional* (paper for the Amsterdam Privacy Congres) Amsterdam 7-10 October 2012.

Finn, Wright & Friedewald 2013

R.L. Finn, D. Wright & M. Friedewald, 'Seven Types of Privacy', in S. Gutwirth, Y. Poullet et al. (eds.), *European Data Protection: Coming of Age*, Dordrecht: Springer 2013.

Fitzpatrick 2004

J. Fitzpatrick, *Human Rights in Crisis: The International System for Protecting Rights During States of Emergency*, University of Pennsylvania Press, 1994.

Foot 2007

R. Foot, 'The United Nations, Counter Terrorism, and Human Rights: Institutional Adaptation and Embedded Ideas', *Human Rights Quarterly* 2007, Vol. 29, No.2, pp. 489–514.

Freeman 2012

Michael Freeman, ed., *Financing Terrorism,: case studies*, Ashgate Publishing, 2012.

Freeman 2013

Michael Freeman and Moyara Ruehsen: *Terrorism Financing Methods: An Overview*, , Perspectives on Terrorism, Vol 7, No 4 (2013).

Friedman 2007

L.M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*, Stanford: Stanford University Press 2007 (blackmail).

Galetta & de Hert 2014

Antonella Galetta & Paul de Hert, '*Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance'* Utrecht Law Review' Volume 10, Issue 1, January 2014 p. 55-75.

Gandy 1993

O. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press: Boulder CO 1993.

L. Gelemerova 2008

L. Gelemerova, *Two years after the Introduction of the US Money Laundering Control Act of 1986*, .'On the Frontline Against Money-Laundering: the Regulatory Minefield', *Crime, Law and Social Change* 2008, Vol. 52, No. 1, pp. 33-55.

Gelemerova 2011

L. Gelemerova, *The Anti-Money Laundering System in the Context of Globalisation: a panopticon built on quicksand?,* Nijmegen: Wolf Legal Publishers 2011, p. 5.

Gellert and Gutwirth 2013

R. Gellert and S. Gutwirth, *Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment*, Prescient. FP 7 project March 2013.

Glendon 1991

M.A. Glendon, *Rights Talk – The Impoverishment of Political Discourse*, New York: Free Press 1991, p. 41.

Glenn 2004

R.A. Glenn, *The Right to Privacy: Rights and Liberties Under the Law*, Santa Barbara 2004.

Golder 2006

B. Golder and G. Williams, 'Balancing National Security and Human Rights. Assessing the Legal Response of Common Law Nations to the Threat of Terrorism', *Journal of Comparative Policy Analysis* 2006, Vol. 8, No. 1, pp. 43-62.

Gordon 2013

G. Gordon, *Innate cosmopolitanism: Mapping a latent theory of world norms in international law*, Ph.D thesis, Amsterdam April 2013.

Green 1967

L. Green, 'Continuing the Privacy Discussion: A Response to Judge Wright and President Bloustein', *Texas Law0020Review* Vol. 46, No. 750, 1967-1968, p. 750.

Greer 1997

S. Greer, *The exceptions to Articles 8 to 11 of the European Convention on Human Rights*, Strasbourg: Council of Europe 1997, pp. 5-40.

Grégr, Kajan, Matoušek & Veselý 2011

M. Grégr, M. Kajan, P. Matoušek & V. Veselý, 'Designing Lawful Interception in IPv6 Networks', in: *Security and Protection of Information*, Brno 2011, <http://www.fit.vutbr.cz/research/view_pub.php?file=%2Fpub%2F9620%2FCLANEKv2.pdf&id=9620>.

Gross 1967

H. Gross, 'The Concept of Privacy', *New York University Law Review* 1967, Vol. 42, No. 34.

Guillaume 2004

G. Guillaume, 'International and Comparative Law Quarterly', *Oxford Journals* 2004, Vol. 53, No. 3, pp. 537- 548.

Habermas 1996

J. Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*, translated by W. Rehg, Cambridge/Massachusetts: The MIT Press 1996.

Habermas 1996

J. Habermas, 'Democratic Theory' in: *Democracy and Difference, Contesting the Boundaries of the Political*, ed. S. Benhabib, Princeton University Press 1996.

De Hert & Papakonstantinou 2014

de Hert, P. J. A. & Papakonstantinou, *' The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition',* *Computer Law and Security Review*. 2014, 30, 6, p. 633- 642.

De Hert 2015

P. de Hert**, '***The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?*' in Merkourios: Utrecht Journal of International and European Law. 31, 80, p. 1-4.

Hesse 1999

K. Hesse, *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*, Heidelberg: C.F. Müller, 1999.

Heymann 2001

P.B. Heymann, 'Civil Liberties and Human Rights in the Aftermath of September 11', *Harvard Journal of Law & Public Policy* 2001-2002, Vol. 25, No. 2.

Higgins 1997

R. Higgins 'The General International Law of Terrorism', in: R. Higgins & M. Flory, *Terrorism and International Law*, London: Routledge 1997, p. 28.

Hirsch Ballin 2012

M. Hirsch Ballin, *Anticipative Criminal Investigation: Theory and Counterterrorism Practice in The Netherlands and the United States*, Utrecht: Universiteit Utrecht 2012.

Van den Hoven van Genderen 2008

R. van den Hoven van Genderen, *Cybercrime investigation and the protection of personal data and privacy*, Strasbourg: Council of Europe 2008.

Van Kempen 2009

P.H. van Kempen, 'The Protection of Human Rights in Criminal Law Procedure in The Netherlands, pre advies Netherlands Comparative Law Association', *Electronic Journal of Comparative Law* 2009, Vol. 13 No. 2.

Konvitz 1966

M.R. Konvitz, 'Privacy and the Law: A Philosophical Prelude', *Law and Contemporary Problems* 1966, Vol. 31, No. 2, pp. 272-280.

Koops 2010

B.J. Koops, 'Het failliet van het grondrecht op dataprotectie', in: J.E.J. Prins (eds.), *16 miljoen BN'ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij 2010, p. 99-110.

Koops 2013

Koops, B.J, *Police investigations in Internet open sources: Procedural-law issues* in: Computer Law & Security Review Volume 29, Issue 6, December 2013, p. 654–665.

Koops 2014

Koops, Bert Jaap, *The trouble with European data protection law*, International Data Privacy Law, 2014, Vol. 4, No. 4.

Korff 2008

D. Korff, *The Sstandard Approach Under Articles 8 – 11 ECHR and Article 2 ECHR*, London Metropolitan University 2008.

Kokott and Sobotta 2012

Juliane Kokott and Christoph Sobotta: *The Kadi Case – Constitutional Core Values and International Law – Finding the Balance?*, The European Journal of International Law Vol. 23 no. 4, 2012.

Kuitenbrouwer 2000

F. Kuitenbrouwer, 'Privacy: een historisch-vergelijkend overzicht', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2000.

Lavery, Johnston & Ludwin 2008

J. Lavery, P. Johnston & S. Ludwin, Proposed Amendments for Public Emergencies in the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans 2008.

Lindzey, Gilbert & Fiske 1954

G. Lindzey, D. Gilbert & S. Fiske, *The Handbook of Social Psychology*, Cambridge Mass.: Addison-Wesley 1954, Vol. 1, 601-36.

Lord Lester, Pannick & Herberg 2004

Lord Lester, D. Pannick and J. Herberg (eds.), *Human Rights Law and Practice*, London: Butterworth 2004, par. 4. 82.

Locke 1960

J. Locke, *Two treatises of Government*, Cambridge: Cambridge University Press 1960 (First edition 1698).

Lyon 1994

D. Lyon, *The Electronic Eye: The Rise of the Surveillance Society*, Minneapolis: University of Minnesota press 1994.

Lyon 2003

D. Lyon, *Surveillance after September 11*, Oxford: Blackwell Publishing Ltd 2003.

Manners 2008

I. Manners, 'The Normative Ethics of the European Union', *International Affairs* 2008, Vol. 84, No. 1, p.45-67.

Hinojosa Martínez 2008

L.M. Hinojosa Martínez, 'The Legislative Role of the Security Council in its Fight Against Terrorism: Legal, Political and Practical Limits'. *International and Comparative Law Quarterly* 2008, Vol. 57, pp. 333-359.

McCloskey 1980

McCloskey, Henry J. "Privacy and the right to privacy." *Philosophy* 55.211 (1980): 17-38.

McClurg 1994

A.J. McClurg, 'Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places', *North Carolina Law Review* 1994-1995, 989 at 995.

McCullagh 2011

D. McCullagh, 'ISP Data Retention Plan Hits Capitol Hill Snag', *CNET* 12 July 2011.

McHarg 1999

A. McHarg, 'Reconciling Human Rights and the Public Interest: Conceptual Problems', *Modern Law Review* 1999, Vol. 62, No. 5, pp. 671-696.

Mill 1869

J.S. Mill, *On Liberty, Chapter I ,Chapter III: Of Individuality, as One of the Elements of Well-Being*, London: Longman, Roberts & Green 1869; Bartleby.com 1999, <www.bartleby.com/130/>.

Moore 2008

A.D. Moore, 'Defining Privacy', *Journal of Social Philosophy* 2008, Vol. 39, No. 3, p. 411-428.

Moss 2007

D. Moss, *A Submission Prepared Exclusively For the Home Affairs Committee in Connection with its Inquiry into a Surveillance Society*, Business Consultancy Services Ltd. 2007.

Muller 2008

M. Muller QC, 'Terrorism, Proscription and the Right to Resist in the Age of Conflict', *Denning Law Journal* 2008, Vol. 20, pp. 111-131.

Murphy 1954

G. Murphy, 'Social Motivation', in: G. Lindzey (Ed.), *Handbook of Social Psychology*, Cambridge Mass: Addison-Wesley 1954, Vol. 1, pp. 601-633.

Newell 1987

W.R. Newell, 'Superlative Virtue: The Problem of Monarchy in Aristotle's 'Politics'', *Western Political Quarterly* 1987, Vol. 40, No. 1, pp. 159-178.

Nicolaidis & Nicolaidis 2004

K. Nicolaidis & D. Nicolaidis, 'The EuroMed beyond Civilisational Paradigms' 2004, in E. Adler, F. Bicchi, B. Crawford and R. Del Sarto (eds), *The Convergence of Civilisations: Constructing a Mediterranean Region*. Toronto: University of Toronto Press 2006.

Nissenbaum 2010

H. Nissenbaum, *Privacy in Context,* Stanford Law Books 2010.

Opsahl 1992

T. Opsahl: 'Articles 29 and 30. The Other Side of the Coin', in A. Eide, G. Alfredsson, Eds., *The Universal Declaration of Human Rights – A Commentary,* Oslo: Scandinavian University Press 1992, p. 459-458.

Parenti 2007

C. Parenti, *The Soft Cage: Surveillance in America, from Slavery to the War on Terror*, Basic Books: New York 2007, p. 200.

Polčák 2012

Structure and Proportionality of Fundamental Rights, Masaryk University Journal of Law and Technology, Vol. 6: 3, 2012.

Polčák 2011

Designing Lawful Interception in IPv6 Networks, Brno University of Technology Faculty of Information Technology.

Prosser 1960

W.L. Prosser, '*Privacy', California Law Review* 1960, Vol. 48, No. 3, pp. 383-423.

Prosser 1971

W.L. Prosser, *The Law of Torts* 1971, par. 118.

Posch 2009

A. Posch, 'The Kadi Case: Rethinking the Relationship between EU Law and International Law?', *Columbian Journal of European Law* 2009, Vol. 15.

Randolph 1893

A. M. F. Randolph, The Trial of Sir John Falstaff.

Reidenberg 1992

J.R. Reidenberg, 'Privacy in the Information Economy: A Fortress or Frontier for Individual Rights', *Federal Communications Law Journal* 1992, Vol. 44, No. 2, pp. 196-197.

Richards & Solove 2010

N.M. Richards & D.J. Solove, 'Prosser's Privacy Law: A Mixed Legacy', *California Law Review* 2010, Vol. 98, p. 1887, Available at: <http://scholarship.law.berkeley.edu/californialawreview/vol98/iss6/5>.

Robertson 1968

A.H. Robertson, 'The United Nations Covenant on Civil and Political Rights and the European Convention on Human Rights', *British Year Book of International Law* 1968-1969, Vol. 43, No. 21, pp. 23-30.

Saul 2005
B. Saul, 'Definition of 'Terrorism' in the UN Security Council: 1985–2004', *Chinese Journal of International Law* 2005, Vol. 4, No. 1, pp. 141-166, par I.

Schauer 1991

F. Schauer, 'Exceptions', *University of Chicago Law Review* 1991, 58, pp. 871-900.

Asser/Scholten Algemeen Deel 1974

P. Scholten, P., *mr. C. Asser's handleiding tot de beoefening van het Nederlandsch Burgerlijk Recht, Algemeen deel*, Zwolle: W.E.J.Tjeenk Willink 1974 (First Edition 1934).

Van der Schyff 2008

G. van der Schyff, 'Cutting to the Core of Conflicting Rights: the Question of Inalienable Cores in Comparative Perspective', in: E. Brems ed., *Conflicts between Fundamental Rights,* Antwerpen: Intersentia 2008, pp. 131-147.

Simoncini 2009

M. Simoncini, 'Risk Regulation Approach to EU Policy Against Terrorism in the Light of the ECJ/CFI Jurisprudence', *German Law Journal* 2009, Vol. 10, No. 11, pp. 1526-1549.

Simpson 2001

A.W. Simpson, *Human Rights and the End of Empire: Britain and the Genesis of the European Convention*, Oxford University Press 2001, p. 715.

Slobogin 2007

Ch. Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment,* University of Chicago Press 2007.

Solove 2001

D.J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven and London: Yale University Press 2011.

Sottiaux 2008

S. Sottiaux, *Terrorism and the Limitation of Human Rights,* Oxford and Portland: Oregon 2008.

Staring 1820

A.C.W. Staring, *De Hoofdige Boer,* 1820. In the Report of the Government, *Data for Action* 2007.

Stone & Warner 1992

M.G. Stone & M. Warner, 'Politics, Privacy and Computers', *The Political Quarterly* 1969, 40, p. 256-260.

Taylor 2002

N. Taylor, 'State Surveillance and the Right to Privacy', *Surveillance and Society* 2002, Vol. 1, No. 1, pp. 66-85.

Vedder, Van der Wees, Koops & de Hert 2007

A. Vedder, L. van der Wees, B-J. Koops & P. de Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw,* Den Haag: Rathenau Instituut 2007, Study 49.

Ten Voorde 2011

J.M. ten Voorde, 'Waakzame burgers beter beschermd?', *NJB* 2011, nr.7.

Walters 2001

G. Walters, *Human Rights in an Information Age: A Philosophical Analysis,* Toronto: University of Toronto Press 2001, p. 159.

Walters 2001

G. Walters, 'Privacy and Security: An Ethical Analysis', *Computers and Society* 2001, Vol. 31, No. 2, p. 9.

Warren & Brandeis 1890

S.D. Warren & L.D. Brandeis, ‘The Right to Privacy’, *Harvard Law Review* 1890, Vol. 4, No. 5.

Weatherill 2011

S. Weatherill, ‘The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court’s Case Law has Become a ‘Drafting Guide’’, *German Law Journal* 2011, Vol. 12, No. 3, p. 828-863.

Wessels 2001

L. Wessels: *Derogation Of Human Rights International Law Standards – A Comparative Study*, University of Johannesburg (thesis) 2001.

Westin 1970

A.F. Westin, *Privacy and Freedom*, New York: The Bodley Head Ltd 1970.

Westin 1970

A.F. Westin, Chapter 1, the Functions of Privacy in Society, the Origins of Modern Claims to Privacy in: Privacy and Freedom, New York 1970.

Whitman 2004

J.Q. Whitman, ‘The Two Western Cultures of Privacy: Dignity Versus Liberty’, *Faculty Scholarship Series* 2004.

Wilson 2005

R.A. Wilson, *Human Rights in the ‘War on Terror’,* Cambridge University Press 2005.

Wisman 2013

T.H.A. Wisman, ‘Purpose and Function Creep by Design: Transforming the Face of Surveillance Through the Internet of Things, *European Journal of Law and Technology* 2013 (2).

Wolff 1990

R.P. Wolff, *The Conflict Between Authority and Autonomy*, Oxford: Basil Blackwell 1990, p. 20.

Wright & Raab 2014

David Wright & Charles Raab (2014) Privacy principles, risks and harms, *International Review of Law, Computers & Technology*, 28:3, 277-298.

Yemin 1969

E. Yemin, *Legislative Powers in the United Nations and Specialized Agencies* (diss. Thèse Genève) 1969.

Zelman 2001

J.D. Zelman, 'Recent Developments in International Law: Anti-Terrorism. Legislation – Part One: An Overview', *Journal of Transnational Law & Policy* 2001, No. 11, pp. 183-200.

Case Law and Other Sources

ECHR 22 February 2013, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. The Netherlands* [2013], App. no. 39315/06.

ECHR 2 December 2010, *Uzun v. Germany* [2010], App. no. 35623/05.

ECHR 14 September 2010, *Sanoma Uitgevers B.V. v. The Netherlands* [2010], App. no. 38224/03, § 66.

ECHR 18 May 2010, *Kennedy v. the United Kingdom* [2010], App. no. 26839/05, § 152, § 90.

ECHR 4 December 2008, *S. and Marper v. the United Kingdom* [2008], §112.

ECHR 1 October 2008, *Liberty and Others v. the United Kingdom* [2008], App. no. 58243/00, § 62.

ECHR 30 January 2008, *Ekimdzhiev v. Bulgaria* [2008], App. no. 62540/00.

ECHR 4 December 2007, *Dickson v. the United Kingdom* [2007], App. no. 44362/04, § 78.

ECHR 26 July 2007, *Peev v. Bulgaria* [2007], App no. 64209/01.

ECHR 10 April 2007, *Evans v. the United Kingdom* [2007], App. no. 6339/05, § 77.

ECHR 6 September 2006, *Segerstedt-Wiberg and Others v. Sweden* [2006], App. no. 62332/00, § 76.

ECHR 29 June 2006, *Weber and Saravia v. Germany* [2006] App no. 54934/00, § 94.

ECHR 24 November 2004, *Aalmoes & Others v. The Netherlands* [2004], App. no. 16269/02, § 7/8.

ECHR 27 August 2004, *Connors v. the United Kingdom* [2004], App. no. 66746/01, § 82.

ECHR 25 December 2001, *P.G. and J.H. v. The United Kingdom* [2001]**,** App. no. 44787/98.

ECHR 22 March 2001, *K.-H.W. v. Germany* [2001], App. no. 37201/97, 36 EHRR 59.

ECHR 18 January 2001, *Coster v. the United Kingdom* [2001], App no. 24876/94, § 104.

ECHR 4 October 2000, *Khan v. the United Kingdom* [2000], App. no. 35394/97, § 26.

ECHR 28 September 2000, *Messina v. Italy (no. 2)* [2000], App. no. 25498/94, § 65.

ECHR 20 June 2000, *Foxley v. the United Kingdom* [2000], App. no. 33274/96, § 43.

ECHR 4 May 2000, *Rotaru v. Romania* [2000], App. no. 28341/95, §§ 43-44.

ECHR 16 February 2000, *Amann v. Switzerland* [2000], App. no. 27798/95, §§ 65-67.

ECHR 30 July 1998, *Valenzuela Contreras v. Spain* [1998], App. No. 27671/95.

ECHR 25 March 1998, *Kopp v. Switzerland* [1998], 27 EHRR 91.

ECHR 30 January 1998, *United Communist Party of Turkey and Others v. Turkey* [1998], 26 EHRR 121, § 43.

ECHR 27 August 1997, *MS v. Sweden* [1997], App. no. 20837/92, 3 EHRR 248.

ECHR 25 June 1997, *Halford v. the United Kingdom* [1997], App. no. 20605/92, § 49.

ECHR 31 January 1995, *Friedl v. Austria* [1995], EHRR 83, App. no. 15225/89.

ECtHR 16 December 1992, *Niemitz v. Germany* [1992], App No. 13710/88.

ECtHR 25 March 1992, *Campbell v. United Kingdom* [1992], A. 233.

ECtHR 26 November 1991, *The Sunday Times v. The United Kingdom (no.2)* [1991], App. no. 13166/87, A 217.

ECtHR 24 April 1990, *Kruslin v. France* [1990], 12 EHRR 546.

ECtHR 22 February 1989, *Barfod v. Denmark* [1989], s.12, para. 29.

ECtHR 26 March 1987, *Leander v Sweden* [1987], 9 EHRR 433, § 48.

ECtHR 17 October 1986, *Rees v United Kingdom* [1986], App. no. 9532/81, 9 EHRR 56.

ECtHR 21 February 1986, *James and Others v UK* [1986], A 98, s. 35, 36, 37, paras 46, 51, 54, 56.

ECtHR 2 August 1984, *Malone v. UK* [1984], 7 EHRR 14.

ECtHR 25 March 1983, *Silver v. the UK* [1983], A. 61, paras. 97-98.

ECtHR 23 September 1982, *Sporrong and Lönnroth* [1982], A 52, s. 26, 28, paras. 69, 73.

ECtHR, *Malone v. Metropolitan Police Commissioner* No. 2 [1979], 2 WLR 700.

ECtHR 26 April 1979, *Sunday Times v. UK* [1979], 2 EHRR 245.

ECtHR 6 September 1978, *Klass and others v. Federal Republic of Germany* [1978], 2 EHRR 214.

ECtHR 7 December 1976, *Handyside v. UK* [1976], A. 24, paras 48-49.

ECHR 21 February 1975, *Golder v. The United Kingdom* [1975], 1 EHRR 524.

ECHR 1 July 1961, *Lawless v. Ireland* [1961], 1 EHRR 15.

Supreme Court (Spain) 25 April 2013, Jyske Bank Gibraltar Ltd v. Administración del Estado [2013].

Supreme Court of The Netherlands (Hoge Raad) 28 September 2010, LJN BM6656 [2010], *NJ* 2010, 532.

Supreme Court of The Netherlands (Hoge Raad) 20 April 2010, LJN BK3369 [2010], *NJ* 2011, 222.
Supreme Court (Bundesverfassungsgericht) 15. December 1983 [1983] 1 BvR 209/83.

Supreme Court (Bundesverfassungsgericht) 3 March 2004 [2004], 1 BvR 2378/98.

Supreme Court (Bundesverfassungsgericht) 2 March 2010 [2010], 1 BvR 256/08.

Supreme Court (Canada) 11 January 2002, *Suresh v Canada* [2002], 1 S.C.R. 3, 2002 SCC 1.

Supreme Court (United States) 16 May 1988, *California v. Greenwood* [1988], 486 U.S. 35.

Supreme Court (United States) 18 December 1967, *Katz v. United States* [1967], 389 U.S. 347.

Supreme Court (United States) 4 juni 1951, *Dennis v United States* [1951], 341 US 494, 524.

Supreme Court (United States) 4 June 1928, *Olmstead v. U.S.* [1928], 277 U.S. 438.

ECJ

Case C-362/14 , 16 October 2015 *Maximillian Schrems v Data Protection Commissioner* [2015].

Cases C-293/12 and C-594/12, 27 January and 28 November 2012, *Digital Rights Ireland Ltd v. Minister for Communications* [2012].

Cases C-92/09 and C-93/09, 9 November 2010, *Schecke and Hartmut* [2010], ECR I-11063.

Case C-28/08, 29 June 2010, *Commission v. Bavarian Lager* [2010], ECR I-06055.

Case C-557/07, 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* [2009], I-01227.

Case C-301/06, 10 February 2009, *Ireland v. European Parliament and Council of the European Union* [2009], ECR I-00593.

Cases C-402/05 & C-415/05, *Kadi & Al Barakaat v. Council of the European Union* [2008], 3 C.M.L.R. 41.

Case C-243/13, 10 February 2005, *European Commission v. Kingdom of Sweden* [2005].

Directives

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, 2.12.2015 COM(2015) 625 final 2015/0281

Directive 2015/849/EC
Directive 2015/849/EC 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 EU L141/73.

Directive 2009/136/EC

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services.

Directive 2006/24/EC

Directive 2006/24/EC 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 [2006] OJ L 105/54 (Data Retention Directive).

Directive 2005/60/EC

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.

Directive 2002/58/EC

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).

Directive 2002/21/EC

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), Consideration 7.

Directive 95/46/EC

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, *Official Journal* L 281, 23 November 1995.

Directive 91/308/EEC

Directive 91/308/EEC of the European Parliament and of the Council of 10 June 1991 on Money Laundering.

Reports

Report on the Mid-Term Review of the Stockholm Programme 2014

L.Berlinguer, J.F. López Aguilar & C. Casini, *Report on the MidTterm Review of the Stockholm Programme* 2014.

Report on the US NSA Surveillance Programme 2013

European Parliament, *Committee on Civil Liberties, Justice and Home Affairs* 2009-2014. Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs.

WODC Report 2012

G. Odinot, D. de Jong, J.B.J. van der Leij, C.J. de Poot & E.K. Straalen, *TheUse of Telephone and InternetTtaps in Criminal Investigations in The Netherlands* (Het gebruik van telefoon- en internettap in de opsporing), WODC Report 2012.

9/11 Commission Report

The 9/11 Commission Report.

HEMOLIA Project 2011

HEMOLIA Project, Hybrid Enhanced Anti-Money Laundering Intelligence, Investigation, Incrimination and Alerts 2011-2014.

Report 01/2010

Report 01/2010 on the Scond Joint Enforcement Action: Compliance at National Level of Telecom Providers and isp's with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the e-Privacy Directive.

Report on Money Laundering 2010

C. Taveres, G. Thomas & M. Roudaut, *Money Laundering in Europe. Report ofWwork Carried out by Eurostat and DG Home Affairs,* Luxembourg: Publications Office of the European Union 2010.

Report 2010

J-M. Dinant, C. de Terwangne & J-Ph. Moiny, *Report on the Lacunae of the Convention for theProtection ofIindividuals with Regard to Automatic Processing of Personal Data (ETS No. 108) Resulting from Technological Developments,* Council of Europe 2010.

Report 2009

M. Scheinin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,* United Nations 2009, A/HRC/13/37.

CTIVD Reports

The Supervisory Commission on the National Security Agencies Report 2009, CTIVD nr. 19-38.

CBP Guidelines 2009

CBP Guidelines, *The Application of Automatic Recognition of License Plates by the Police* 2009.

Report Commissie Datastromen en Veiligheid 2007

Commissie Datastromen en Veiligheid, *Gegevensbestanden voor veiligheid: observaties en analyse,* NCTb 2007.

SECILE Report 2007

The EU Data Retention Directive: a Case Study in the Legitimacy and Effectiveness of EU Counter-Terrorism Policy, SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness. A Project co-funded by the European Union within the 7th Framework Programme – Security Theme.

OECD guidelines 1980
OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 1980.

EDPS
EDPS, Opinion 8/2015 Dissemination and use of intrusive surveillance technologies

Regulations

Regulation of the European Parliament and of the Council, (COD) 2012/0011 of 25 January 2012 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2012].

Council Regulation (EC) 2001/2580 of 27 December 2001 on Specific Restrictive Measures Directed Against Certain Persons and Entities With a View to Combating Terrorism [2001] OJ L344/70.

Council Common Position 2001/931/CFSP of 27 December 2001 on the Application of Specific Measures to Combat YTerrorism [2001] OJ L344/93.

Charter of Fundamental Rights of the European Union 2000/C of 18 December 2000 Official Journal of the European Communities [2000] C 364/1.

Working Document 2012

European Parliament 9 October 2012 Working Document 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 [2012], PE491.322v01-00.

A Framework for Program Assessment 2008

Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals: Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment 2008, p. 9, <http://epic.org/misc/nrc_rept_100708.pdf>.

FATF Recommendations, IX Special Recommendations 2012

The Financial Action Task Force Recommendations 2012 - International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.

Increasing Resilience in Surveillance Societies Project 2012

Increasing Resilience in Surveillance Societies, To investigate Societal Effects of Different Surveillance Practices From a Multi-Disciplinary Social Science and Legal Perspective 2012-2015, Deliverable D1.1: Surveillance, Fighting Crime and Violence December 2012.

Principles 1984

United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities, Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights 1984, Annex, UN Doc E/CN.4/1984/4.

Proposed Amendments for Public Emergencies in the Tri-Council Policy Statement 2008

J. Lavery, P. Johnston & S. Ludwin, Proposed Amendments for Public Emergencies in the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans 2008, <http://www.pre.ethics.gc.ca/policy-politique/initiatives/docs/Public_Emergencies_March_2008_-_EN.pdf>.

The White House 2014

The White House, ‘Big Data: Seizing Opportunities, Preserving Values’, *Whitehouse.gov* 1 May 2014.

The White House 2014

The White House, ‘Remarks by the President on Review of Signals Intelligence’, *Whitehouse.gov* 17 January 2014.

Webwereld 2014

Ch. Koenis, ‘Justitie: afplakken webcam heel verstandige zet’, *Webwereld.nl* 15 January 2014, <http://webwereld.nl/beveiliging/80911-justitie-afplakken-webcam-heel-verstandige-zet>.

Der Blog des Arbeitskreises Vorratsdatenspeicherung 2013

Michael, ‘Frau Malmström und die ‘Expertengruppe’’, *Blog.vorratsdatenspeicherung.de* 15 May 2013.

Rijksoverheid 2012

Rijksoverheid, ‘Opstelten wil opsporing op internet versterken’, *Rijksoverheid* 16 October 2012, <http://www.rijksoverheid.nl/nieuws/2012/10/16/opstelten-wil-opsporing-op-internet-versterken.html>.

UK Human Rights Blog

A. Wagner a.o., ‘Article 8, Right to Private and Family Life’, *ukhumanrightsblog.com.*

New York Post 2010

Post Staff Report, ‘Italian Court Convicts Google Execs over Online Video’, *New York Post* 2010, <http://nypost.com/2010/02/24/italian-court-convicts-google-execs-over-online-video/>.

European Parliament 2010

Press release European Parliament: Information Society, *Internet of Things and Governance*, June 15 2010, (Ref: 20100614IPR76044). Available at: <http://www.europarl.europa.eu/sides/getDoc.do?language=nl&type=IM-PRESS&reference=20100614IPR76044>.

Business Consultancy Services 2007

D. Moss, *A Submission Prepared Exclusively for the Home Affairs Committee in Connection with itsIinquiry into a Surveillance Society* by David Moss of Business Consultancy Services Ltd. 2007, <http://dematerialisedid.com/BCSL/HAC3.pdf>.

2012: Requests for Retained Data: Age of Data when Requested

Age of data requested (months)	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Not specified	Total
Belgium										
Bulgaria									91 159 (1083)	91 159 (1083)
Czech Republic	48 972 (7581)	4539 (1831)	720 (1794)	2104 (110)						56 335 (11 316)
Denmark	4375	1232	532	305	181	32	13	8		6678
Germany										
Estonia	1561 (427)	910 (371)	925 (167)	773 (366)						4149 (1331)
Ireland	6415 (257)	1034 (329)	589 (30)	325 (32)	87	123	105 (12)	145 (1)	6 (2)	8829 (664)
Greece									28 313 (3026)	28 313 (3026)
Spain										
France										
Italy										
Cyprus										
Latvia										
Lithuania	14 555	6681	294 (1878)	35 (10)						21 565 (1888)
Luxembourg										
Hungary										
Malta										
The Netherlands										
Austria										
Poland	1 111 243	287 342	101 762	64 333	42 633	28 738	21 917	60 147	(44 505)	1 718 115 (44 505)
Portugal										
Romania										
Slovenia	793	248	112	42	31	5	3		43 (1)	1277 (1)
Slovakia										
Finland	2196	1489	976	376	497				(497)	5534 (497)
Sweden										

United Kingdom	255 886	20 545	9664	12 027					426 652 (716)	724 751 (716)
Total	**1 445 996 (8265)**	**324 020 (2531)**	**115 574 (3869)**	**80 320 (518)**	**43 429**	**28 898**	**22 038**	**60 300**	**546 173 (49 831)**	**2 666 725 (65 027)**

2011: Requests for Retained Data: Category of Data

Category	Fixed network telephony	Mobile telephony	Internet-related	Not specified	Total
Belgium					
Bulgaria	24086 (517)		24 500 (151)	25 710 (708)	74 296 (1376)
Czech Republic	6370 (179)	111 759 (17 117)	4556 (1720)		122 685 (19 016)
Denmark	191	3801	243		4235
Germany					
Estonia	1477 (1030)	807 (25)	1529 (283)		3813 (1338)
Ireland	3525	5062 (2)	4101		12 688 (2)
Greece					
Spain					
France					
Italy					
Cyprus	1	43	22 (2)		66 (2)
Latvia	981 (157)	34 816 (330)	3246 (535)		39 043(1022)
Lithuania	376(14)	26 887 (1858)	513		27 776 (1872)
Luxembourg		87			87
Hungary					
Malta					
The Netherlands					
Austria					
Poland				1 856 915 (17 219)	1 856 915 (17 219)
Portugal					
Romania					
Slovenia				1473 (6)	1473 (6)
Slovakia	158 (62)	30 204 (88)	689 (164)		31 051 (314)
Finland				5331 (221)	5331 (221)
Sweden					
United Kingdom				728 852 (786)	728 852 (786)
Total	**37 165 (1959)**	**213 466 (19 420)**	**39 399 (2855)**	**2 618 281 (18 940)**	**2 908 311 (43 174)**

Table 1: Purpose Limitation for Data Retention Stated in National Laws	
Estonia	May be used if collection of the evidence by other procedural acts is precluded or especially complicated and the object of a criminal proceeding is a criminal offence [in the first degree or an intentionally committed criminal offence in second degree with a penalty of imprisonment of at least three years][21].
Ireland	For prevention of serious offences [i.e. offences punishable by imprisonment for a term of 5 years or more, or an offence in schedule to the transposing law], safeguarding of the security of the State, the saving of human life.[22]
Greece	For the purpose of detecting particularly serious crimes[23].
Spain	For the detection, investigation and prosecution of the serious crimes considered in the Criminal Code or in the special criminal laws[24].
France	For the detection, investigation, and prosecution of criminal offences, and for the sole purpose of providing judicial authorities with information needed, and for the prevention of acts of terrorism and protecting intellectual property[25].
Italy	For detecting and suppressing criminal offences[26].
Cyprus	For investigation of a serious criminal offence[27].
Latvia	To protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings[28]
Lithuania	For the investigation, detection and prosecution of serious and very serious crimes, as defined by the Lithuanian Criminal Code[29] .
Luxembourg	For the detection, investigation, and prosecution of criminal offences carrying a criminal sentence of a maximum one year or more[30].
Hungary	To enable investigating bodies, the public prosecutor, the courts and national security agencies to perform their duties, and to enable police and the National Tax and Customs Office to investigate intentional crimes carrying a prison term of two or more years[31].