DATA PROTECTION LAW: RECENT DEVELOPMENTS

(Settore scientifico-disciplinare: IUS/13; IUS/14)

DOTTORANDO: DEDE KASNECI
COORDINATORE DEL COLLEGIO DEI DOCENTI: CHIAR. MO. PROF. ALBERTO GASPARINI
UNIVERSITÀ DI TRIESTE

FIRMA:

RELATORE: CHIAR. MO. PROF. DORIS HATTENBERGER
UNIVERSITÀ DI KLAGENFURT

FIRMA:

ANNO ACCADEMICO 2008/2009
In loving memory of my father
Abstract

The purpose of this PhD thesis is to analyze the legal background, the recent developments and the current challenges of the Data Protection Law, with a particular focus on the European Data Protection Law, notably the Directive 95/46/EC, which will be analyzed in detail.

The data protection rules originally developed, at national level in the 1970s, as a response to the threats posed to the privacy by the technological developments of the 1960s and 1970s. At the EC level, the first legal instrument in this field was Data Protection Directive, which was passed in 1995 to harmonize national data protection laws within the European Community, with the aim of protecting the fundamental rights and freedoms of individuals including their privacy and personal data.

After 15 years the question is whether the Data Protection Directive 95/46/EC fit the objectives for which it was adopted in 1995. The European Commission considers that the Directive 95/46/EC fulfils its original objectives and therefore does not need to be amended. This thesis questions this static approach of the European Commission to the data protection regime and argues that the increasing pressure on privacy due to the development of privacy destroying technologies and the growing use of and demand for personal information by public and private sectors, requires quick legal answer and constant change of the data protection legislation.

The research carried out for this thesis shows that, over time the social and regulatory environment surrounding the creation, management and the use of personal data has evolved significantly since the adoption of the Directive 95/46/EC. The Directive is showing its age and is failing to meet the new challenges posed to privacy by factors such as the huge growth of personal information on line and the growing availability and ability of the new technologies to process, use and abuse personal information in many ways.

These factors have challenged the means and the methods used by Directive to protect personal data and have altered the environment for the implementation of the Directive. Thus, it is clear that the context in which the data protection Directive was created has been changed fundamentally and certain basic assumptions of the Directive have already been challenged in approach, in law and in practice. All these factors show that the Directive is out of touch to meet the technological, social and legal challenges of 21st century and therefore need to be reviewed and amended.
Keywords

Data protection law
Data subject
Data controller
Data processor
Data Protection Authority (DPA)
Information Technology
Informational privacy
Privacy
Passenger Name Record “PNR”
Technology neutrality
# Table of Contents

Abstract .......................................................................................................................... iii

Keywords ....................................................................................................................... iv

List of Abbreviations ..................................................................................................... ix

1  Introduction ................................................................................................................ 1
   1.1 Problems of privacy and data protection: concepts in disarray ......................... 1
   1.2 Problems with the European Data Protection Law: an outdated legal framework in need of review ................................................................. 7
   1.3 Objectives, research questions and the methodology of the thesis .................... 10
   1.4 A road map for this thesis ................................................................................... 11

2  The origin and the development of the data protection law .................................... 14
   2.1 The problem: development of the computer technology poses threats to privacy 14
   2.2 The early response at the national level: first national laws on data protection 15
   2.3 Response at the International Level: OECD, Council of Europe and UN ............ 16
      2.3.1 OECD Guidelines on the Protection of Privacy (1980) ......................... 17
      2.3.2 Council of Europe Convention No.108 (1981) .................................. 18
      2.3.3 UN Guidelines concerning the computerized data Files (1990) ............. 19
   2.4 Response at the regional level: EU Law and APEC privacy framework ............ 19
      2.4.1 EU Data Protection Directive (1995) ................................................... 20
      2.4.2 APEC Privacy Framework (2004) ....................................................... 21
   2.5 Criticism of the data privacy regimes ................................................................. 21

3  Current challenges posed to privacy and data protection .................................... 23
   3.1 Theoretical challenge: different understandings of Privacy ............................... 23
   3.2 Technological challenge: privacy destroying technologies .............................. 27
      3.2.1 The limits of the claim for technological neutrality ............................... 28
   3.3 Increased pressure on privacy by public and private sectors ............................. 30
      3.3.1 “Public-and-private-partnership” on EU level ........................................... 30
         3.3.1.1 Data Retention Directive ................................................................. 30
         3.3.1.2 API Directive .............................................................................. 31
         3.3.1.3 EU-PNR ..................................................................................... 31
      3.3.2 Private-public-partnership on International level ..................................... 33
         3.3.2.1 Passenger Name Record (PNR) case ............................................. 33
         3.3.2.2 SWIFT Case .............................................................................. 34
   3.4 Information Governance ..................................................................................... 35
   3.5 Legal Challenge: construction of a global data protection regime .................... 35
European Data Protection Law: a fragmented legal framework between the First and the Third Pillars

Inter-pillar demarcation of competence in the field of data protection

Demarcation of competence between the Pillars: Article 47 EU Treaty

Choice of Pillar in the field of data protection law: ‘PNR’ and Data Retention Directive Cases

Data Protection Law in the First Pillar

Data Protection Directive 95/46/EC

Regulation (EC) No. 45/2001 on the protection of personal data by Community Institutions


Data Retention Directive: a controversial measure

Additional Data Protection-related Instruments in the First Pillar

Data Protection in the Second Pillar (CFSP): no harmonized standard governing data protection

Specific data protection provisions

Framework Decision 2008/977/JHA: a “police cooperation” document or a “data protection” text?

Changes in the Lisbon Treaty: New horizons for the data protection in the European Union?

Legal Analysis of the Data Protection Directive 95/46/EC

Conflicting Objectives

Principles

Controller’s obligations versus data subject rights

Transfer of data to non-EU countries

Country Adequacy

Legal Problems with the Directive 95/46/EC

Difficulty in applying legal definitions [Article 2]

The definition of the controller [Article 2(d)]

“Data Controller” versus “Data Processor”

The need to add some definitions to the Directive

Problematic aspects of the “Applicable Law” [Article 4]
6.2.1 Problems with applicable law between the EU Member States [Article 4(1)(a)] 71
6.2.2 Problems with applicable law between the EU and Non-EU countries [Article 4(1)(c)] 72
6.2.3 Problems with the wording of Article 4(2) ............................................................. 73
6.3 Reconciling Data Protection with Freedom of Expression [Article 9] .................. 74
6.4 Data Subject rights to object [Article 14(a)] ............................................................... 75
6.5 Problems with data-flow to third countries [Articles 25 and 26] ....................... 76
   6.5.1 The Directive does not define the concept of “transfer” of personal data....... 77
   6.5.2 Problematic aspects with country “adequacy” .................................................. 79
   6.5.3 Limits of “Consent” as a criterion for legitimizing the data processing/transfer [Article 26(1)] ............................................................................................. 80
   6.5.4 Limits of the “appropriate contractual clauses” [Article 26(2)] ................. 82

7 Initiatives for the review of the Data protection Directive 95/46/EC .............. 83
   7.1 Evaluation of the Directive 95/46/EC by the EU Commission: Amendments premature .................................................................................................................. 83
   7.2 Past initiatives for the review of the Directive 95/46/EC: Sweden “Misuse Model” of data protection ........................................................................................................ 84
   7.3 The current voices calling for the review of the Directive 95/46/EC............ 86
      7.3.1 European Data Protection Supervisor ............................................................. 89
      7.3.2 The UK Information Commissioner’s Office (ICO) ........................................ 90

8 Tentative solutions to the legal challenge: Prospects for the construction of a
global data protection regime .................................................................................. 92
   8.1 Promoting factors for a regulatory consensus on data protection at the global level 93
      8.1.1 The creation of international instrument: a growing need for a global approach 94
      8.1.2 International flow of data from the EU and the US: Safe Harbour privacy principles. .......................................................... 95
      8.1.3 Directive 95/46/EC: A soft mechanism of legal globalization............... 96
      8.1.4 2005 Montreux Declaration of Data Protection Commissioners: working towards adopting a Universal Convention on Data Protection ........................................... 97
   8.2 Slowing down factors for regulatory consensus on data protection at the global level 98
8.2.1 Lack of any clear and generally agreed definition of privacy ............................ 98
8.2.2 Differences between the data protection regimes: the divide between the EU and the US .......................................................................................................................... 98
8.2.3 The lack of a strong representative International body to adopt rules ............. 99
8.3 Conclusion: It is difficult to achieve a regulatory consensus at global level on data protection .......................................................................................................................... 100
8.4 Two tentative solution from the EU data protection perspective: Harmonization on regional level and extraterritoriality ................................................................. 100
8.4.1 Harmonization on regional level ...................................................................... 101
8.4.2 Claiming extraterritoriality of the EU data protection law .............................. 101
8.4.2.1 Extraterritoriality in the EU Data Protection Laws ...................................... 102
8.4.2.1.1 Extraterritoriality of the Directive 2002/58/EC .................................... 103
8.4.2.1.2 “Single economic entity” doctrine in EU Law .................................... 105
8.4.2.1.3 The “Implementation doctrine” in the EU Law .................................. 106
8.4.2.1.4 The ‘effect doctrine’ in EU Law ..................................................... 107
8.4.2.2 Compatibility of privacy laws which have extraterritorial effects with the WTO Rules .................................................................................................................. 110
9 Conclusions and recommendations ....................................................................... 114
9.1 Conclusions ........................................................................................................ 114
9.2 Recommendations ............................................................................................... 119
9.2.1 Recommendations of essential importance ................................................... 119
9.2.2 Recommendations that are advisable but not essential ............................... 124

Bibliography ............................................................................................................. 126

ANNEX I: Data protection laws worldwide ............................................................. 139

ANNEX II: 2007 Agreement between the EU and US on the processing and transfer of passenger name record (PNR) data by air carriers to the US Department of Homeland Security (DHS) .............................................................. 143
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APEC</td>
<td>Asia Pacific Economic Cooperation</td>
</tr>
<tr>
<td>API</td>
<td>Advanced Passenger Information</td>
</tr>
<tr>
<td>CIS</td>
<td>Custom Information System</td>
</tr>
<tr>
<td>CMLR</td>
<td>Common Market Law Reports</td>
</tr>
<tr>
<td>CMLRev.</td>
<td>Common Market Law Review</td>
</tr>
<tr>
<td>CLJ</td>
<td>Cambridge Law Journal</td>
</tr>
<tr>
<td>CFI</td>
<td>Court of First Instance</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>EC</td>
<td>European Community</td>
</tr>
<tr>
<td>ECLR</td>
<td>European Competition Law Review</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>ECJ</td>
<td>European Court of Justice</td>
</tr>
<tr>
<td>ECR</td>
<td>European Court Reports</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ELJ</td>
<td>European Law Journal</td>
</tr>
<tr>
<td>E.L.Rev.</td>
<td>European Law Review</td>
</tr>
<tr>
<td>ICO</td>
<td>UK Information Commissioner’s Office</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>PET</td>
<td>Privacy Enhancing Technologies</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification Devices</td>
</tr>
<tr>
<td>RTDE</td>
<td>Revue Trimestrielle de Droit Européen</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>RMUE</td>
<td>Revue du Marché Unique Européen</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunication</td>
</tr>
<tr>
<td>SIS</td>
<td>Schengen Information System</td>
</tr>
<tr>
<td>29 WP</td>
<td>Article 29 Working Party</td>
</tr>
<tr>
<td>W.T.O.</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>
1 Introduction

“A society that will trade a little liberty for a little order will lose both, and deserve neither”

Thomas Jefferson

1.1 Problems of privacy and data protection: concepts in disarray

Privacy and data protection concern everyone and are issue of profound importance around the World. Numerous commentators have declared privacy as “essential to democratic government”, necessary for “permitting and protecting an autonomous life” and important for “emotional and psychological tranquility”. Privacy has been hailed as “an integral part of our humanity” the “hart of our liberty” and “the beginning of all freedoms”. Given its importance, privacy is recognized as a fundamental human right according to many International Instruments such as: the United Nations Universal Declaration of Human Rights of 1948 (Article 12), International Covenant on the Civil and Political Rights (Article 17) The European Convention of Human Rights of 1950 (Article 8), the Charter of Fundamental Rights of the European Union of 2007 (Article 8) and the Treaty of Lisbon of 2008 (Article 16 of the TFEU).

Furthermore, Multinational Privacy Guidelines, Directives, and frameworks have influenced the passage of laws on privacy and data protection in a vast majority of nations. In 1980 the Organization for Economic Cooperation and Development (OECD) issued its Privacy Guidelines. In 1981 the Council of Europe adopted the Convention Nr.108 on data protection. In 1990 the UN adopted the Guidelines concerning the computerized data files. In 1995, the European Union adopted the Data Protection Directive 95/46/EC and in 2004 the Asia-Pacific Economic Cooperation (APEC), set forth a privacy framework. Furthermore, thousand of laws in nearly every nation seek to protect privacy around the world. The vast majority of nations protect privacy in their constitutions.

However, beyond this worldwide consensus about the importance of privacy and data protection and the need for their protection, there is confusion about the concept of privacy. The current understanding of informational privacy is based to some extent on how

an individual relates to and control access to information about themselves\(^2\). The word ‘privacy’ means the people’s right not to have sensitive information about them shared without their consent or an overriding legal reason. Regulations and legislation have codified what Judge Samuel Warren Louis Brandeis summarized in 1890 as the right of the individual to “be let alone”\(^3\) and expanded the notion of data protection beyond the fundamental right to privacy.

**Privacy is still a concept in disarray**\(^4\). Privacy is a contested legal concept, with several understandings and more misunderstandings, covering distant areas of human activities\(^5\). Privacy is actually shorthand for a complex bundle of issues, ranging from dignity to discrimination, and rooted in our need to control what we tell others about ourselves. Thus, it is difficult for philosophers, legal theorists and lawyers to reach a *satisfying conceptualization of the privacy*.

The difficulty to reach a *satisfying conceptualization of the privacy* is due to a range of reasons. **First of all**, some authors contend that privacy can be socially detrimental. Legal scholar, Fred Cate declares that privacy is “an antisocial construct ... [that] conflicts with other important values within the society, such as the society interests in facilitating free expression, preventing and punishing crime, protecting private property and conducting government operations effectively”\(^6\). **Second**, various nations or regions (ex. USA, EU and APEC), even though they accept privacy as a valuable social interest, they put different values on the notion of privacy, which causes considerable uncertainty about exactly which values and interests are promoted by privacy and data protection laws.

**Third, the main reason for the difficulty and the inconsistency in the definition of privacy is that there are some eternal privacy tensions**, namely, the interests protected by privacy and data protection laws are inherently in conflict with other legitimate interests such as the freedom of speech, public security and the free flow of information.

**On the one hand, it is impossible to belong to a community and withhold all data.** Every encounter reveals details about us, whether it is a social encounter, a professional one, a consumer experience or a citizenry political act. We leave traces of information with our


\(^4\) SOLOVE, *supra note 1*.


\(^6\) SOLOVE, *supra note 1*.
friends, employers, consultants, service provider’s shops and governments with who we may be in daily contact. When we buy a product we reveal who we are our specific interests and how much we pay for it. The data is used to create commercial profiles. Using these profiles, merchants want to charge rich customers more, and governments want to tax rich citizens more. Therefore, Data and Information both in public and private sector has become the new raw material of the world economy. Just as in the past centuries iron, wood and coal were foundation upon which the economy was based, so nowadays it is data and information. The accumulated data is a valuable asset for those who collect it. Once the data is obtained it is an independent asset that other companies (and governments) might be interesting in acquiring 7.

The new possibilities of processing data easily and cheaply may serve to improve the efficiency of businesses and government services and might benefit consumers and citizens who enjoy personalized services and prefer to be identified than to be treated as part of the mass.

On the other hand, the collection and the processing of our data carry with it many risks and dangers. There is increasing concern about the social consequences and the dangers of processing the personal data of individuals, and confusion about where the line should be drawn between the economic benefits of data processing and the dangers to personal privacy and liberty which this may bring. One such risk is that the data will be abused by those who access it, either by authorization or not. Data which was consensually provided for one purpose might be used against us in a different context. For example, genetic data about one’s risks of suffering from cancer one day might be the basis for the insurance company to deny its services or increase the premium paid. Or, data provided to a school about specific needs of a student might be referred to at a later date to deny employment.

The difficulty in articulating what privacy is and why it is important to protect causes a lot of legal problems. First of all, the privacy is frequently misconstrued or inconsistently recognized in law, which fails to identify the central interests at stake which the privacy law is asked to redress. Second, we frequently lack a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems. Therefore, since legal protection of privacy depends upon a conception of privacy that informs what matters are protected and the nature and scope of the particular protections

7 BIRNHACK, supra note 5, p.3.
employed, the lack of a clear concept of what exactly privacy is creates difficulties when making policy, and as a result the legislation fail to pass both at the national level and most importantly at the global level. For the same reason, even when the privacy laws are passed, the lack of clarity makes the privacy laws ineffective and blind to the larger purposes it must serve.

**Other privacy tensions are driven by technology which gave rise to the emergence of the data protection law**: the falling cost of data storage and communication makes it easier for merchants and governments to collect more data on people and thus to become more efficient to violate the privacy. The development of the Computer technology in the 1960’s and 1970’s and the enormous potential of the digital revolution made the civil libertarians worry. The nightmare of all-seeing, all-knowing “Big Brother” of George Orwell’s “1984” did not belong anymore to the realm of the fiction, but was a reality. And as the enormous potential of the digital revolution became more apparent and together with it the dangers posed to privacy, so the calls for the specific measures to protect individuals became louder.

**The right to data protection emerged in Europe, as a legal response to the threat posed to the privacy and identity of the individuals by the mass processing of the information.** It emerged as a new legal field in the early 1970s, separate from the *privacy law* but dependent upon it. The new field followed the growth of the information technologies and globalization processes. Ever since the evolution of the data protection law underwent several stages corresponding to new privacy challenges. Every new stage of data protection law first at the national level (Land of Hesse Germany 1970) and then at the International level (1980 OECD Guidelines, 1981 Council of Europe Convention) and EU level (Directive 95/46/EC) was a response to the new threats that the development of the computer technologies continuously pose to privacy and data protection.

**Europe has proven to be the leader in protecting privacy and personal data of the individuals in the digital age.** While the US approach considers the data protection a sub-category of privacy, the alternative legal approach chosen in Europe for the regulation of personal data is a *sui generis protection*, which is not a sub-category of privacy law but is a close legal neighbour thereto. Thus European law has recognized that data is *important per se*. This difference derives from the fact that the value placed upon privacy in the US and EU varies considerably from each-other. While in Europe the problem of controlling the personal data is a matter of human dignity which deserves a *sui generis* protection, in the US

---

8 BIRN Hack, *supra note 5*, p. 6.
the data protection is a sub-category of the right to privacy, understood in the background of liberty and of free flow of information. Thus, the European privacy law protects dignity, while American privacy law protects liberty.

In addition to the technological and philosophical factors, determinative for the emergence of the data protection laws in Europe, were also the ideological factors and the historical ones. Concerns of privacy tend to be high in societies espousing liberal ideals. The development of legal regimes for privacy protection is most comprehensive in the western democracies. By contrast such regimes are under-developed in most African and Asian nations. However, in the USA—often portrayed as the citadel of the liberal ideals—the legal respect for privacy falls short in significant respects of the protection levels offered in other countries, notably Member States of the EU. However, this variation between the US and Europe, can be attributable - at least in part- to differences in perceptions of the degree to which privacy is or will be threatened. The comprehensive data protection framework in Europe undoubtedly reflects the traumas from the experience of totalitarian oppressions (i.e. Nazism and Communism).

Today, the concern about the privacy and data protection remains largely the same as before. The general trend is driven by the technological innovation and by economic and social forces creating a demand for privacy-destroying technologies. The rapid development of privacy-destroying technologies by governments and businesses threatens to make data protection obsolete. Therefore, headlines such as “the death of privacy” have unsettled consumers and given rise to fears that, we have entered “a new world” in which personal liberty is a thing of the past.

Data Protection is still under constant attack from many different angles. The continuous technological developments, the relentless demands of the global markets and the pressing security needs, especially in the aftermath of the 9/11 September is posing new threats to the privacy and data protection both within the EU and outside its borders. The globalization of information exchange and personal data processing, the complexity of systems, the potential harms derived from the misuse of more and more powerful

---

10 BYGRAVE (2004), supra note 9, p.328.
11 BYGRAVE (2004), supra note 9, p.329.
13 FROOMKIN, supra note 12.
technologies, the shift of government *agendas* from freedom and privacy interests to security considerations after 9/11 September are posing new threats to privacy. Following the lost of millions of confidential data in the UK and Germany, more and more data protection authorities and civil society organizations have become aware of the danger that the disclosure of personal information involves\(^{15}\). Therefore, numerous commentators have declared that privacy is “*under siege*” or “*dead*”. As Professor Deborah Nelson has put it, “Privacy, it seems, is not simply dead. It is dying over and over again”\(^{16}\). In 2007 the Privacy International in its yearly reports found out that “*there is a worsening of privacy protection across the world, reflecting an increase in surveillance and a declining performance of the privacy safeguards*”\(^{17}\).

Actually, among others three are the main challenges that the data protection is facing: first the theoretical-political challenge, second, the technological challenge and third the legal challenge.

**The theoretical challenge:** As there is no theoretical or political consensus on privacy, we encounter different legal approaches to privacy. The divide between the US and Europe is a stark example. Therefore the first privacy challenge is choosing the best understanding of privacy.

**The technological challenge:** As computer technology becomes progressively powerful and more use is made of computers, the dangers are set to increase. As the technology will continue to outpace the imagination of the cleverest law-makers, it is a challenge for law-makers to adopt laws to keep pace with the advances in rapidly changing circumstances.

**The legal challenge:** Since privacy is understood differently in the US, Europe and elsewhere, and that the legal category of information privacy (i.e. data protection) is not recognized as such in many countries the question raised is: what should be the global legal regime? Although international instruments such as OECD Guidelines have shown their importance in the world-wide protection of personal data, they are not sufficient as such to safeguard a comprehensive and appropriate personal data protection in the context of digital economy\(^{18}\). Therefore, the future legal challenge is to narrow the gap between the USA and


\(^{16}\) SOLOVE, *supra note 1*.

\(^{17}\) Privacy International 2009.

Europe and to construct a viable global legal regime that would provide data subjects with control over the personal data and at the same time allows trans-border flows.

1.2 Problems with the European Data Protection Law: an outdated legal framework in need of review


The Directive 95/46/EC is also seen as a unique form of soft legal globalization. The data protection laws of other countries (Australia, Hong Kong, Israel, Japan etc.) and regions (Americas, Asia) are modeled after the EU Directive, which is acknowledged as the main engine of an emerging global legal regime on data protection. Thus, knowledge of how the data protection is regulated in Europe is useful in predicting how other regions may deal with the subject as well.

The Directive 95/46/EC is already 15 years old and the social environment surrounding the use of personal data has significantly evolved at EU and global level since the adoption of the Directive and new social and technological challenges are posing new threats to privacy. The main question is whether the Directive, with its roots in a largely static and less globalized environment, stands up with the challenges of today. To address this question two overarching issues need to be examined:

- First, does the Data Protection Directive fit the objectives for which it was adopted in 1995?
- Second, can the Directive 95/46/EC as currently stands, retain its so far global influence?

The Commission evaluation of the Directive issued in 2007 stressed that the rules of the Directive 95/46/EC are substantially appropriate, they fulfill the original objectives and thus the Directive does not need to be amended.

---

19 BIRNHACK, supra note 5.
However, many other authoritative voices from many quarters do not share this positive assessment of the Commission about the Data Protection Directive. There are growing fears that the Directive 95/46/EC is no longer fit for purposes for which it was adopted in 1995. When the directive was adopted, 15 years ago, the intention was not to create a legal framework, which was well adjusted to take on future data protection and privacy challenges, but, rather to harmonize the existing regulations and to create a common European market for the free movement of personal data. Therefore, the European data protection law is increasingly seen as out of date, bureaucratic and excessively prescriptive. The Directive is showing its age and is failing to meet new challenges to privacy, such as:

- the transfer of personal data across international borders (*Passenger Name Records ‘PNR’ case*\(^{21}\)),
- the increasing availability and ability to process large quantities of data and the huge growth in personal information online,
- the growing demand for and use of personal information, by the public and private sectors,
- the use and abuse personal information in many ways.

These factors all drive and influence each other, serving to alter the environment for the implementation of the Data Protection Directive. The fluidity of the personal data collections has increased to a point that could not have been imagined at the time of the adoption of the Directive. It is thus clear that the context in which the Data Protection Directive was created has changed fundamentally and certain basic assumptions of the directive have already been challenged.

**Moreover, Lisbon Treaty which entered into force on 1 December 2009 brings about important changes and opens new horizons for the data protection in EU.** The right to the protection of the personal data is enshrined in Article 16 of the Treaty on the Functioning of the European Union (TFEU). The upgrading of the right to the protection of the personal data, to a fundamental right laid down in the EU primary law, marks an important and visible change in the direction of an increased protection of this right in the EU. This change in the primary law of the EU will also require changes in the secondary legislation, including the Directive 95/46/EC.

---

Against this background, commentators and various stakeholders believe that the European Data Protection law needs to be modernized in order to meet the technological and social challenges of the 21st century as well as to retain its position as a leading force for the globalization of data protection.

In his opinion of 25 July 2007 on the implementation of the Data Protection Directive 95/46/EC the European Data Protection Supervisor (EDPS) suggested to start the thinking about a future framework on data protection. Several activities have been employed since, either or not inspired by this suggestion:

The Commission installed an Expert Group on Personal Data and on 19 and 20 May 2009 organized a Conference on Personal Data.

European Privacy and Data Protection Commissioner’s Conference held at Edinburgh on 24 April 2009 discussed this issue and called for the start of the debate for the review of the Directive.

The UK Information Commissioner (ICO) commissioned RAND Europe, an independent think-tank, to conduct a review of EU data protection law. The Technical Report published by this think-tank point out many weaknesses of the Directive and suggests its review.

Therefore, the data protection has risen sharply up the political and public agendas and there is increased interest for research and knowledge in this field of law. Moreover, it is acknowledged that the regulation of the data processing and data flows is destined to remain one of the most important regulatory and policy issues of the 21st century. Thus, the research for this thesis comes at a high profile time for privacy and data protection and it attempts to make a contribution, however small, to that debate.

In this context the thesis questions the current static and formal approach of the European Commission to the Data protection law and sustains that the EU current data protection

---

25 RAND Europe (2009), supra note 2.
26 KUNER, supra note 14.
regime is badly equipped to cope both with the new challenges posed to privacy in an evolving information society and to retain its so far global impact as a source of inspiration of data protection laws. Accordingly, the thesis adds another voice to the call for the review of the Directive 95/46/EC, based on the following assumptions:

• the evolving character of information governance and technology and the increasing pressure on privacy, requires quick answer and constant change of data protection law.

• if the Directive is to exert its principles at global level more efficiently, the directive need to be reviewed and streamlined to meet the new challenges.

1.3 Objectives, research questions and the methodology of the thesis

The thesis’ objective is fourfold, first, to analyze the recent developments of the regulatory framework for data protection at EU and global level, secondly, to investigate the weaknesses of the Directive 95/46/EC, thirdly, to look at some avenues for the future improvements in the context of the future review of the Data Protection Directive and fourthly to analyze the prospects for the construction of a viable global legal regime for data protection.

These objectives require a mix of backward-looking and forward-looking research which is focused to answer the following legal research questions:

• Does the speed of the technological changes require new regulatory approaches for the data protection law?

• To what extent the rules laid down in the Directive 95/46/EC fit the purposes for which were adopted in 1995?

• Are the existing rules of the EU data protection law adequate to cope with the new privacy challenges in an evolving information society? If not, what are the weaknesses of the current EU data protection law?

• Is the Directive 95/46/EC a leading legal globalizing force in the emerging global legal regime on data protection, and if so, does the EU legal regime, as it currently stands has the ability to bring the Non-EU member States legal regimes on Data Protection in line with its preferred model?
The methodology used to answer these questions is the review of the relevant legislation, case-law and literature in the field of the EU data protection law, complemented with the interview with experts and stakeholders in the field of the national and EU data protection law. While the thesis has mainly a legal orientation, sometimes its approach is also cross-disciplinary.

1.4  A road map for this thesis

The thesis is structured in nine chapters. In order to understand better the right to data protection and its today challenges, it begins by considering in chapter two, the origin and the development of the Data protection law as a sui generis right. It is argued that Europe has proven to be the leader in protecting the privacy of individuals in the digital age. The data protection emerged in Europe in the early 1970’s, as a legal response to the threat posed to the privacy and identity of the individuals by the mass processing of the information. The next sections of this chapter analyzes also the evolution of the data protection laws which underwent three stages: first, the recognition that the data protection requires regulation at the national level, secondly a shift from national level to international legal regime and thirdly, a shift from an emphasis on the collection of data to the trans-border transfers of such data. This chapter ends with a critical assessment to the data protection regimes in general.

Chapter three analyzes the current challenges that the data protection is facing. It is argued that Data Protection is still under constant attack from many different angles: the globalization of information exchange and personal data processing, the rapid development of privacy-destroying technologies by governments and businesses and the shift of government agendas from freedom and privacy interests to security considerations after September 11, are posing new threats to privacy. This chapter analyses the main challenges that privacy and data protection are facing and how the EU data protection stands up with them. In this context are analyzed the theoretical-political challenge (different understandings of privacy), the technological challenge (development of privacy-destroying technologies), the increased pressure on privacy by the public and private sectors (including the public-and-private partnership for the exchange of data) and the legal challenge (construction of global regime on data protection).
The complex legal framework for data protection at the EU level is analyzed in chapter four. This chapter considers first the criteria elaborated by the ECJ for the demarcation of pillars in the field of data protection and next analyzes the various legal instruments of data protection in the framework of First and Third pillars. In the framework of the First Pillar are analyzed the Data Protection Directive 95/46/EC (considered as *lex generalis*) and other sectoral directives (*lex specialis*), which detail the rules and principles laid down in the Directive 95/46/EC. In the framework of the Third Pillar is analyzed the Framework Decision 2008/977/JHA for the protection of the personal data in the Third Pillar (considered as *lex generalis*) and other specific data protection rules (*lex specialis*) incorporated in various legal instruments of the Third Pillar. It is argued that this fragmentation of the European data protection law under Pillars lines rise many issues. At the EU level, it raises not only Institutional issue of the choice of Pillars which results in useless “tug-of-war” between EU institutions on where to draw the line between the pillars, but also, the issue of consistency and effectiveness of the EU data protection rules, which results in serious gaps for the European data protection regime. This chapter ends with an analysis of the welcomed changes that the Lisbon Treaty brings about for the data protection law.

**Chapter five explains the essential legal concepts of the Directive:** the objectives of the Directive, its principles, the data subject rights, controller’s obligations as well as the export of the personal data from the EU to third countries.

**Chapter six discusses the legal difficulties and problems arising in the text of Directive 95/46/EC.** It is argued that Data Protection Directive has many legal problems. Some of its current rules are too complex and *too strict at a general level* (resulting in excessively stringent regulation beyond what is necessary to counter misuse), while others are *too vague and open-ended* (causing legal uncertainties and differences in application). This chapter analyzes the legal issues that arise under six Articles of the Directive, Article 2 (Definitions), 4 (Applicable law), 9 (freedom of expression), 14 (data subject right to object), Articles 25 and 26 (data-flow to third countries). These legal problems arising from the Directive are analyzed against the wider technical and legal backgrounds.

**Chapter seven examines the recent developments in the context of the review of the Directive 95/46/EC.** It looks first at the European Commission evaluation of the Directive and next it deals with the past (Sweden “misuse model” of data protection) and the current initiatives (European Data Protection supervisor, UK Informational Commissioner’ Office-ICO) undertaken for the Review of the Directive.
Chapter eight offers tentative solutions to address the legal challenge. In this context it attempts to analyze the possibilities of constructing a global data protection law regime. It is argued that many factors and variables promote or slow down the construction of a global data protection regime. However, the analysis demonstrated that it is doubtful that we will see, at least in the short term, major progress with respect to harmonization of the data protection legal regime at the global level. It is argued that this is due not only to the lack of a clear definition of the privacy and the stark divide between the EU and the USA privacy regimes, but also to the lack of a sufficiently strong dynamic and representative International body to bridge these differences (such the WTO). Since the negative scenario (i.e. the slowing down factors) are likely to prevail in the short and medium term, the thesis, propose some alternative solutions to tackle the legal challenge. It is argued that, from the EU data protection point of view, two tentative solutions can be envisaged: first, the regional harmonization, that is, to bring the data privacy regimes of non-EU countries in line with its preferred model and the second solution is to claim the extraterritoriality of the EU law, that is, extending the Extraterritoriality of the EU data protection rules, even though it would remain politically controversial and would raise the problem of enforceability of the decisions.

The Last chapter (ninth) presents the conclusions drawn from the research in question as well as makes some modest recommendations in the context of the review of the Data Protection Directive 95/46/EC.
2 The origin and the development of the data protection law

“The background and the underlying philosophy of the European Directive differ from that of the United States. While there is a consensus among democratic society that information privacy is a critical element of civil society, the US has, in recent years left the protection of privacy to market rather than law. In contrast Europe treats privacy as a political imperative anchored in fundamental human rights.”

Reidenberg, 2001

To understand better the right to data protection and its today challenges, a short history of the origin and of the development of this sui generis right is necessary. Europe has proven to the leader in protecting the privacy of individuals in the digital age.

Data protection emerged in Europe as a new legal field in the early 1970’s, separate from the privacy law, but yet dependent upon it. The new field followed the growth of the information technologies and globalization processes. The evolution of the data protection laws underwent several stages, corresponding to the three privacy challenges, first, the very emergence of the EU data protection law and the recognition that the data protection requires regulation, secondly a shift from national level to international legal regime and thirdly, a shift from an emphasis on the collection of data and its initial processing to subsequent uses and transfers to third parties including trans-border transfers.

2.1 The problem: development of the computer technology poses threats to privacy

The data protection is understood as a legal response to a real problem: the threat posed to the privacy and identity of the individuals by the mass processing of the information. The development of the computer technology in the sixties and seventies and the power of the

---

27 BIRN Hack, supra note 5, p. 6.
28 Ibid.
early big mainframe computers made the civil libertarians worry. The nightmare of allseeing, all-knowing “Big Brother” of George Orwell’s “1984” did not belong anymore to the realm of the fiction, but was a reality. And as the enormous potential of the digital revolution became more apparent and together with it the dangers posed to privacy, so the calls for the specific measures to protect individuals became louder. The development of the data protection passed through many stages, and every new stage of this new law, first at the national level and then international and EU Level was a response to a new threat that the development of computer technologies continuously posed to the privacy and data protection.

In addition to the technological factors, determinative for the emergence of the data protection laws, were the ideological and historical factors. Concerns of privacy tend to be high in societies espousing liberal ideals. The liberal affection for privacy is amply demonstrated in the development of legal regimes for privacy protection. These regimes are most comprehensive in the western democracies. By contrast such regimes are underdeveloped in most African and Asian nations. However, in the USA-often portrayed as the citadel of the liberal ideals-the legal respect for privacy falls short in significant respects of the protection levels offered in other countries, notably Member States of the EU. However, this variation between the US and Europe, can be attributable-at least in part- to the differences in the extent to which persons in respective countries can take for granted that others will respect their privacy. In other words, it can be attributable to differences in perceptions of the degree to which privacy is or will be threatened. The comprehensive data protection framework in Europe undoubtedly reflects the traumas from the experience of totalitarian oppressions (Nazism and Communism).

2.2 The early response at the national level: first national laws on data protection

The initial political interest in the data protection was local in several states. Data protection emerged as a new legal field in the early 1970’s, separate from the privacy law, but yet dependent upon it. The world’s first data protection law was adopted in 1970 in

---

30 BYGRAVE (2004), supra note 9, p.328.
31 Ibid.
32 Ibid. p.329.
German State of Hesse\textsuperscript{33}. The growing opportunities to manipulate individual behaviour through sophisticated processing of personal data were cited as the justification for the law\textsuperscript{34}. Other European nations (Sweden, France etc.) adopted similar data protection laws. Numerous countries around the world have enacted data protection law, but the bulk of these countries are European. The common points of departure for national data protection regimes in Europe are as follows\textsuperscript{35}:

\begin{itemize}
\item Coverage of both public and private sectors,
\item Coverage of both automated and manual systems for processing personal data,
\item Application of broad definitions of “personal data”,
\item Application of extensive procedural principles some of which are rarely found in data privacy elsewhere,
\item Restriction on trans-border flows of personal data,
\item Establishment of independent data privacy agencies with broad discretionary powers to oversee the implementation of data privacy rules,
\item Channeling of privacy complaints to these agencies rather than to courts,
\item Little use of industry-developed codes of practice.
\end{itemize}

The bulk of these characteristics were typical for data protection law in Western Europe. But, due to the EU Directive, they are now also typical for the laws of the Eastern European Countries after accession or candidate. Also other non-EU countries (ex. Canada, Argentina) have adopted the EU approach.

\section*{2.3 Response at the International Level: OECD, Council of Europe and UN}

The growing interest in data protection then shifted to the international level. By the beginning of the 1980s it was becoming apparent that the personal data processing was not confined to isolated mainframe computers, but it was becoming increasingly based around

\begin{flushright}
\textsuperscript{34} BAINBRIDGE, supra note 29, p.14.
\textsuperscript{35} BYGRAVE (2004), supra note 9, p.339.
\end{flushright}
networks. While some of such networks were entirely located within one country, others were international in nature. The new setting presented a fresh challenge for the national regulators seeking to secure a measure of protection of their national citizens. The national law on data protection was becoming obsolete: how could compliance with a national law be ensured when only a small part of a much bigger global network was located in home territory and when the companies or organizations responsible for the running of the network were based abroad? The risk was to create “data heavens” because the problem was becoming too big to be resolved only with national laws. By the end of 1980s, it has become therefore clear that an international solution to the question was required. In 1980 the OECD adopted Guidelines on the protection of privacy and trans-border flows of Personal Data and in 1981 the Council of Europe adopted Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

### 2.3.1 OECD Guidelines on the Protection of Privacy (1980)

As the title of the OECD Guidelines indicates, the shift from the national to the international level highlighted the need for addressing transborder data flows. These guidelines are also significant from another perspective they represent the first Trans-Atlantic Agreement relating to the privacy protection. The Guidelines were intended to harmonize the national privacy legislation and to provide a framework for facilitating the international flows of data. Eight basic principles were adopted providing for collection limitation, data quality, purpose specification, use limitation, security safeguards, openness individual participation and the accountability of the data controller.

The Guidelines were not binding on the OECD Member States, but, its basic privacy principles have been very influential on the drafting of data privacy laws and standards in Europe (Council of Europe and EU) and non-European Jurisdictions such as, Australia, New Zealand, and Canada. Further, they constituted a point of departure for the adoption of the APEC Privacy Framework in 2004. All these instruments, which mirrored the basic principle

---

39 LEVIN, A, and JO NICHOLSON, M., “Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground”, 2005, p.375.
of the OECD Guidelines, increased the legal significance of the principle, notably, when the EU Directive on the Protection of Privacy was adopted some fifteen years later\textsuperscript{40}.

\subsection{2.3.2 Council of Europe Convention No.108 (1981)}

As regards the Council of Europe, article 8 of the ECHR enumerates explicitly privacy as a fundamental human right. In 1950 this right was conceived mainly as the \textit{protection of the intimacy} and intended to ensure \textit{the protection of sensitive data}. Progressively the right to privacy has become the \textit{right to self determination}. It means the possibility for everyone to determine him or herself the way by which he would like to find his or her way in the society\textsuperscript{41}.

At the Council of Europe, this extension of the right to privacy from protection of sensitive data to the right to self determination is done using two avenues: First, the notion of privacy laid down in Article 8 of the ECHR is defined and interpreted broadly by the European Court of Human Rights case-law\textsuperscript{42}. This extension has been made possible because the convention is deemed as “\textit{a living instrument}”, which ought to be interpreted only in an extensive way\textsuperscript{43}. It leads progressively to consider that the protection of all data; what might be viewed as “the information image of the individuals” has to be insured and not only the sensitive ones.

Secondly, besides the broad definition of the scope of the “privacy” right by the European Court of Human Rights, in 1981 the Council of Europe adopted the \textit{Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention No.108}. The convention set out basic privacy principles and provided a template for countries without data protection legislation. The convention provides for eight principles for the automatically processed personal data. It requires that data are obtained and processed fairly and lawfully, stored for specific and legitimate purposes, not used in a way that is incompatible with those purposes, adequate, accurate, preserved for no longer than is required, protected by security measures and that data are accessible to individuals to check their veracity.

\textsuperscript{40}LEVIN and JO NICHOLSON, supra note 39, p.375.
\textsuperscript{43}See on these points notably the \textit{Case Tyrer v. UK}, Judgement of 25 April 1978, § 31 and \textit{Case Selmouni v France} Judgement of 28 July 1999, § 100.
These principles have been the foundation of subsequent privacy regulation in Europe, and beyond. However, Convention 108 has a fundamental problem which concerns the enforceability of the convention itself and the international data processing 44.

2.3.3 UN Guidelines concerning the computerized data Files (1990)

The OECD and the Council of Europe paved the way for other international initiatives. In 1990 the UN published Guidelines Concerning Computerized Data Files 45. The Guidelines are intended to encourage enactment of data privacy laws in UN Member States lacking such legislations. The Guidelines are also aimed at encouraging international organizations to process data in a responsible, fair and privacy-friendly manner. On the matter of trans-border data flows, the UN Guidelines adopt the principle of reciprocity. Their adoption underlines that data privacy is not simply a “First World” Western concern. Moreover, in some respects, the principles in the UN Guidelines go further than some of the other international instruments. However, the Guidelines seem to have had little practical effect relative to the OECD Guidelines and other instruments 46. UN Guidelines lack the binding force and the procedures for implementing them are left to the initiatives of each State 47.

2.4 Response at the regional level: EU Law and APEC privacy framework

Despite the fact that the OECD and Council of Europe instruments paved the way for other international initiatives they have many limitations. For the OECD Guidelines the main problem was their non-binding nature and for the Convention 108, the fundamental problem concerns the enforceability of the convention itself and the international data processing 48. In early 1990s was the time, for the EC to enter in the field, resulting in 1995 in the data protection Directive 49.

44 BAINBRIDGE, supra note 29, p.17.
46 BYGRAVE (2004), supra note 9, p.335.
47 BIRNHACK, supra note 5, p.7.
48 BAINBRIDGE, supra note 29, p.17.
49 BIRNHACK, supra note 5, p.7.
2.4.1 EU Data Protection Directive (1995)

Within the European Community, the European Parliament adopted resolutions in 1976, 1979 and 1982 calling the Commission to propose a directive to harmonize the data protection law. However, the Commission response was initially limited only to a recommendation, requiring the EC Member States to ratify the Council of Europe Convention 108, before the end of the year 1982. But, the Commission saw that the Convention 108 was not an effective and sufficient means of producing a level playing field of data protection law. It became also obvious that data protection is not only an issue of human rights, but also had important implications for trade. The economic activity had become more dependent on the processing of personal data.

These developments and the general climate of enthusiasm for the internal market harmonization led the European Commission to propose in September 1990 a general framework directive to harmonize the national legislation of the Member States. The Directive was adopted in 1995, after five years of difficult negotiation, and came into force in 1998. It was based on the OECD Guidelines, the principles of the Convention 108 and the UN Guidelines, but, specified them and added new elements.

Although the Directive was adopted in 1995, it was rooted in the period before the internet and the information society in general, was firmly established in Europe. After 14 years, the context in which the Directive was created has changed fundamentally and certain basic assumptions of the Directive have already been challenged. This leads to the question: is the current Directive well-adjusted to address the risks posed to privacy today?

Of all instruments analyzed above the EU Directive have become the leading trendsetter and benchmark for data protection around the world. However, if the Directive is to exert its principles at global level more efficiently, it needs to be reviewed and streamlined to meet the new challenges.

---

50 BAINBRIDGE, supra note 29, p. 23.
51 BAINBRIDGE, supra note 29, p. 23.
2.4.2 APEC Privacy Framework (2004)

The alternative to the Directive is the regional framework of the Asia-Pacific Economic Cooperation (APEC), which in 2004 initiated a privacy framework (APEC 2004)\(^{53}\). As the preamble of the privacy framework indicates it is based on the OECD Guidelines\(^ {54} \). The APEC framework provides for nine privacy principles: preventing harm, integrity of personal information, notice, security safeguards, collection limitations, access and correction, uses of personal information, accountability and choice.

Like the OECD, Council of Europe and EU, the APEC’s baseline is the dual goals of protecting privacy and enabling information flows\(^ {55} \). However, while balancing information privacy and business needs, APEC declares its distinctive approach in that it accords “due recognition to cultural and other diversities that exists within its member economies”. Therefore it allows flexibility in implementing the principles.

The APEC privacy framework lacks regulation of cross border data flows, other than an indirect accountability duty and a 2007 mid-proposal for data transfers within APEC. The APEC Privacy Framework is weaker than the EU Directive and is less ambitious in scope, and thus subject to criticism. However, the emergence of the APEC Privacy framework makes it more difficult for the EU to win the challenge at the global level as a super power of data protection.

2.5 Criticism of the data privacy regimes

All the above mentioned data protection legal regimes have their limitations and weak points. In this context, account should be taken of several strands of legitimate criticism of data privacy regimes generally. This critique can be summarized in three lines of criticism.

One line of criticism concerns the regimes’ underdevelopment of a systemic focus—as manifested, for instance in the paucity of direct legislative encouragement for Privacy-Enhancing Technologies (PETs).

Another line of criticism relates to the marginalization of the judiciary. In many countries the courts have played little, if any, direct role in developing and enforcing data


\(^{54}\) See, Preamble of the APEC Privacy Framework, supra note 53, point 5.

\(^{55}\) BIRNHACK, supra note 5, p.7.
privacy norms⁵⁶. This situation not only results in scarcity of authoritative guidance on the proper interpretation of the relevant legislation, but also contributes to the marginalization of the privacy as a field of law.

**A third line of criticism, is that data privacy regimes so far have tended to operate with largely procedural rules that do not seriously challenge the established patterns of information use**, but seek merely to make such use more efficient, fair, and palatable for the general public⁵⁷. Lawmakers’ motives for enacting data privacy laws are increasingly concerned with engendering public acceptance for new information systems, particularly in the electronic commerce. Concomitantly, it is argued that the regimes are incapable of substantially curbing the growth of mass surveillance and control. Although, the criticism is valid, it should not be overlooked, that some regimes-particularly in Europe- have shown an ability to restrict certain data processing practices and to raise the awareness of the importance of privacy safeguards. Nevertheless, the dykes erected in the name of privacy have seldom been high and thick. More ominously, in an ideological climate dominated by the “war on terrorism” the prospects for building new dykes, let alone reinforcing the existing ones, are far from promising⁵⁸.

3  Current challenges posed to privacy and data protection

“Everywhere one turns these days it seems that the right to privacy is consistently under assault”

Bruno Bettelheim, 1968

Privacy and Data Protection is still under constant attacks from many different angles. The globalization of information exchange and the shift of government agendas from freedom and privacy interests to security considerations are posing new threats to privacy. Among others, three are the main challenges that the privacy and data protection are facing: the theoretical-political challenge, the technological challenge and the increased pressure on privacy from the private and public sector. This chapter analyzes these risks and how the Directive 95/46/EC stands up with them.

3.1  Theoretical challenge: different understandings of Privacy

Privacy is a contested legal concept, with several understandings and more misunderstandings, covering distant areas of human activities. Since there is not theoretical or political consensus on privacy we encounter different legal approaches to privacy. The divide between the US and Europe is a stark example. While in EU, there is a broad consensus that the data protection principles should be embodied in a comprehensive law, applicable to all sectors of economy, in the US there is absence of an overall privacy framework, resulting in sector-specific data protection laws. This difference derives from the fact that the value placed upon privacy in the US and EU varies considerably from each-other. While in Europe the problem of controlling the personal data is a matter of human dignity which deserves a sui generis protection, in the US the data protection is a sub-category of the right to privacy, understood in the background of liberty and of free flow of

---

59 BIRNHACK, supra note 5, p. 1.
61 BIRNHACK, supra note 5, p. 2.
information. Thus, the European privacy law protects *dignity*, while American privacy law protects *liberty*.62

In US the privacy evolved in two different realms: the public sphere and the private one.63 In the public sphere, privacy emerged as a constitutional right, protecting citizens against the government encroachment. In the private realm, privacy emerged as a common law right, but, limited to certain categories. The category of *information privacy (data protection)* is not included. As a result, the US has adopted *ad hoc*, sectoral approach to the data protection, based on whether the collector of the data is the government or the private player.

**Besides the above legal-historical explanation, there are several other possible explanations for the US skepticism towards recognizing a general data protection right**. The first (political) explanation concerns the US tradition of limited government, which enables to regulate the public sector extensively but, generally prevents the federal government from limiting interaction between the citizens.65 The second (political-economic) explanation concerns the fact that personal data is seen as a tradable asset in its own, and thus the regulation of the data is conceived as an unwarranted intervention in the market.66 A third explanation is that in the US there is skepticism about restriction on the free flow of information.67 Privacy and data protection restricts the dissemination of information and thus harms the free speech interests.

**The alternative legal approach chosen in Europe for the regulation of personal data is a sui generis protection**, which is not a sub-category of privacy law but is a close legal neighbour thereto.68 The European law has recognized that *data is important per se* whether it is the government who collects and processes it or the private players in the market. The initial focus is not on the identity of the data controller (USA approach) but on the interest of the *data subjects*. **Thus, in Europe data protection form a separate body of rules which derives from the privacy and the idea of the human dignity**.69 As a result, the EU tackles

---

63 BIRNHACK, supra note 5, p.2.
64 BIRNHACK, supra note 5, p.3.
66 BIRNHACK, supra note 5, p. 3.
67 MAXEINER, supra note 33, p.94.
68 Ibid. p.3.
69 Ibid. p.4.
the data protection through enacting a comprehensive legislation such as the Directive 95/46/EC.

The different approaches of EU and US on data protection rules gave rise to disputes between the two jurisdictions over the transfer of data (*PNR*\(^{70}\) and *SWIFT* cases\(^{71}\)). While the US government is subject to data privacy laws\(^{72}\), it is the lack of a concerted regulation in the private sector that the Commission will not recognize the US as a “safe” country\(^{73}\). A compromise was reached in 2000 through the “Safe Harbour” Agreement\(^{74}\). However, this solution was questionable not only due to its self-regulatory nature and the lack of the actual effectiveness, but also due to the fact that rights and interests of the European citizens have been pushed to one side\(^{75}\). Furthermore, the Safe Harbour Principles are challenged by the *PNR* and the *SWIFT* cases.

**Since the privacy is understood differently in the EU, US and elsewhere, it follows that, the first privacy challenge is choosing the best understanding of privacy.**

From the EU data protection standpoint this challenge is twofold: first, how to retain the so far global impact as a worldwide preferred model of data protection law, and second, how to achieve greater harmonization with the US data protection regime.

Concerning the first challenge, the Directive 95/46/EC is credited so far with success because the data protection laws of many non-European countries are modeled under the EU model\(^{76}\). However, to meet this challenge for the EU will be more difficult in the future for two reasons, first because of the recent emergence of A.P.E.C\(^{77}\) as a potential competitor in the role of the data privacy “superpower” and second because of the current weaknesses of the Directive 95/46/EC, notably its Articles 25 and 26\(^{78}\).

The second challenge is also very difficult. Even though the privacy is protected less in the US than in Europe, it is not very realistic to expect that the US, the sole economic superpower and the current dominant of the Internet (more than 60 percent of the websites

\(^{70}\) *PNR* case, supra note 21.

\(^{71}\) Society for Worldwide Interbank Financial Telecommunication (SWIFT).

\(^{72}\) Privacy Act 1974.

\(^{73}\) REID, *supra note* 60, p.495.


\(^{75}\) REID, *supra note* 60, p. 496.

\(^{76}\) BIRNHACK, *supra* note 5.

\(^{77}\) APEC Privacy Framework, *supra* note, 53.

\(^{78}\) BYGRAVE (2004), *supra note* 9, p. 495.
are located in the US\textsuperscript{79}, reform its data privacy law so as to comply with the European approach\textsuperscript{80}.

Three possible solutions can be envisaged to tackle this challenge: First, the ideal solution would be to negotiate a Universal Convention on Data Protection. This solution was put forward by the Declaration of the International Conference of Data Protection and Privacy Commissioners, adopted in 2005 at its 27\textsuperscript{th} conference\textsuperscript{81}. In the Montreux declaration, the Privacy and Data Protection Commissioners:

- Agree to collaborate with governments, international and supranational organizations for the development of a Universal convention for the protection of the Individuals with regard to the processing of their personal data,

- Appeal to the UN to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights,

However, even though this declaration is an important promoting factor to develop a universal convention for the data protection, many other factors slow down the construction of a global data protection regime. The lack of a clear and generally agreed definition of what privacy means and the differences between the US and EU on the data protection regimes are the main factors which makes extremely doubtful to achieve, at least in the short term, major progress with respect to harmonization of data protection law at the global level.

From the EU data protection point of view remains two other solutions: \textbf{first, the regional harmonization}, that is, to bring the data privacy regimes of non-EU countries in line with its preferred model\textsuperscript{82}. \textbf{The second solution is the extraterritoriality} of the EU data protection law that is, extending the extraterritorial application of the EU data protection rules, even though it would remain politically controversial and would raise the problem of enforceability of the decisions\textsuperscript{83}. These options will be analyzed further in the last chapter.

\textsuperscript{79} POULLET, supra note 41, p. 13.
\textsuperscript{80} BYGRAVE, (2004), supra note 9, p.348.
\textsuperscript{81} “Montreux Declaration “The protection of personal data and privacy in a globalized world: a universal right respecting diversities” adopted by the International Conference of the Data Protection and Privacy Commissioners at its 27\textsuperscript{th} International Conference, held from 14- to 16 September 2005.
\textsuperscript{82} BYGRAVE (2004), supra note 9, p. 348.
\textsuperscript{83} REID, supra note 60, p. 489.
3.2 Technological challenge: privacy destroying technologies

The emergence of the information technologies posed a new challenges to privacy\textsuperscript{84}. The technology provides the opportunity to use and misuse personal information in unique ways and is always evolving: what is exciting today is commonplace tomorrow\textsuperscript{85}.

However, the Directive 95/46/EC seems out of touch with the recent technological developments. Since the adoption of the Directive in mid-1990s until today, there have been considerable developments not foreseen by the directive. It is not an exaggeration to say that the internet has transformed the world we live in\textsuperscript{86}. In Europe the use of internet was not widespread before the time of the adoption of the directive. The text of the directive refers only to general terms such as “information society” “information technology” but, does not even mention the term “Internet”. One can argue that, this was done to draft a technologically neutral measure, but this is not a plausible reason, because none of the articles of the Directive were designed with the internet in mind\textsuperscript{87}. Accordingly, the Directive seems unable to cope with the size and the trans-national nature of the Internet.

The Directive is based on the assumption of static data processing purposes and controllable information flows\textsuperscript{88}. The Directive is fitted for a world with only mainframe computers and central databases, where transfers between the computers could easily be blocked. Thus, the current explosion of the global communications and the spread of the global information networks was not anticipated by the Directive. Therefore, it is hard to see how the directive can be applied to the current non-frame technologies that decentralize the use of data. The micro-management envisaged by the Directive is impossible with today information and communication technology.

Accordingly, since the development in technology is threatening the individual privacy, the challenge for the EU data protection law is to keep up with the fast pace of technological changes. Unless social, legal or technological forces intervene, it is conceivable that there will be no place on earth where ordinary person will be able to avoid surveillance\textsuperscript{89}.

\textsuperscript{84} BIRNHACK, supra note 5, p. 4.
\textsuperscript{85} RAND Europe (2008), supra note 52, p.12.
\textsuperscript{86} REID, supra note 60, p.489.
\textsuperscript{87} REID, supra note 60, p.493.
\textsuperscript{88} RAND Europe (2008), supra note 52, p.16.
\textsuperscript{89} FROOMKIN, supra note 12.
3.2.1 The limits of the claim for technological neutrality

One of the arguments given by the European Commission in a Communication (2007) on the follow-up of the Work Programme for better implementation of the Directive 95/46/EC for not amending it is that “the Directive is technologically neutral”\(^{90}\). The principle of technological neutrality was coined officially by the European Commission in 1999\(^{91}\).

However, the claim of technological neutrality is questionable both from philosophical and legal perspectives. From a philosophical perspective (i.e. interplay between the society and technology), individuals who consider technology as neutral see technology as neither good nor bad and what matters are the ways in which we use technology\(^{92}\). However, technology is only neutral if it’s never been used before, or if no one knows what it is going to be used for\(^{93}\). But, obviously, “such a society is non-existent and once becoming knowledgeable about technology, the society is drawn into a social progression where nothing is ‘neutral about society’”\(^{94}\).

The principle, in the legal context means that the legal framework is not limited to a specific technological context\(^{95}\), so that new laws do not need to be passed every time a new technology is invented. However, technological neutrality in the legal context is a questionable principle, because it brings vagueness and creates legal uncertainty. Moreover, in the data protection law it is very difficult to sustain this principle at all.

The technological developments are never neutral\(^{96}\). We need to acknowledge that changing technological environments alter the habitat of a policy. New policies need to reflect the totality of the new environment. Data protection law requires that the legal innovation follows technological novelty. The increased ease with which personal data collected and further processed, as such, creates an increased threat to the rights and interests of data.

\(^{93}\) Supra note 90.
\(^{94}\) Supra note 90.
\(^{95}\) RAND EUROPE (2009), supra note 2, p. 24.
subjects. This rise will continue exponentially, posing serious challenges to the capability of regulators. The new technologies challenge the old concepts.

This is demonstrated by the following example: For instance, the 18th recital of the preamble of the e-Commerce Directive (2000)\textsuperscript{97} says that:

“activities which by their very nature cannot be carried out at a distance and by electronic means, such as… medical advice requiring the physical examination of a patient are not information society services”

This statement is already simply untrue because doctors can already and will increasingly in the future carry out “physical examinations” of the patients at a distance\textsuperscript{98}. One can also bring other more recent examples in this respect. It is the European Commission itself that acknowledges that the technological progress make the old articles outdated obsolete. For example in the Explanatory Memorandum for the Proposal of the E-Privacy Directive\textsuperscript{99}, European Commission (2007) explains that:

“Article 3(2) and (3) [of e-Privacy Directive 2002] are deleted as redundant. Because of technological progress, the exceptions justified by technical impossibility or the disproportionate economic effort will be rendered obsolete”

These examples shows that it is very difficult for the data protection law be technologically neutral, because the new technologies require quick answer, i.e. change of laws, otherwise they risk to become obsolete due to the technological developments.

Accordingly, the European Commission should accept the limits of the technological neutrality claim for the data protection law, and recognize that the evolving character of technological environment requires that the data protection law be in constant change and modernized through legal innovations.


3.3 Increased pressure on privacy by public and private sectors

The public and private sector are exerting tremendous pressure on privacy. The personal data is an important tool in the hands of businesses vis-à-vis both current and potential customers. Similarly, in the public sector, the sharing of personal data is regarded as an enabler to support the achievements of certain objectives such as the delivery of existing or new services.

In the post-9/11 world, policymakers in several countries have tipped the balance in favour of national security over individual privacy. The governments are collecting, monitoring and using personal information for anti-terrorism and law enforcement purposes.

Moreover, there is increasingly cooperation between the public and private sector both on EU level (Data Retention Directive, API Directive and EU-PNR) and International level (EU-USA PNR, SWIFT), where companies are increasingly becoming agents of governments. This is eroding the previously clearly defined responsibilities between the public and private sectors and is an example of a situation where convergence of functions can lead to diminished trust and increased risks of privacy threats. These new threats posed to privacy by the public and private partnerships are considered more in detail in the following sections.

3.3.1 “Public-and-private-partnership” on EU level

The public-private-partnership on the EU level is exemplified by three cases, Data Retention Directive, the EC Directive 2004/82/EC on the passenger data and the draft for a framework decision to use PNR data for law enforcement purposes.

3.3.1.1 Data Retention Directive

Data Retention Directive 2006/24/EC, adopted in 2006, provides for the obligation of the Member States to require from the communication providers to retain communication data for a period of between 6 months and 2 years. While the main reason for the adoption of this Directive, i.e. to combat terrorism and organized crime, sounds justified, its adoption has
raised many concerns and creates considerable legal gaps and uncertainty for the data protection law. These shortfalls of this controversial measure will be analyzed more in detail in chapter 4, (section 4.2.4).

### 3.3.1.2 API Directive

Another striking example of public-private-partnership on the EU level is Directive 2004/82/EC on the obligation of carriers to communicate advanced passenger data, which was adopted in 2004 in the wake of the Madrid bombings. The so-called API (Advanced Passenger Information) system includes, among others information about names, data of birth, passenger number, nationality, the initial point of embarkation of flight passengers and other elements (Article 3(2)). According to Article 1 “This Directive aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities”. Two remarkable exceptions to the original purpose of the Directive are made in Article 6(1): Firstly, it is provided that data shall be deleted within 24 hours after transmission “unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks”. Secondly, Member States may also use the personal data for law enforcement purposes. These exceptions are not necessarily covered by the Directive original aim. Using data for law enforcement purposes leads to data processing out of the scope of combating illegal immigration and improving border control. Recital 6 expressly states that “Under these exceptional circumstances the Directive should be adopted without the opinion of the European Parliament.”

API Directive also raises many concerns and creates considerable legal gaps and uncertainty for the data protection law at the EU level.

### 3.3.1.3 EU-PNR

Inspired by the EU-USA PNR Agreement (see Annex II) and in relation to the above mentioned API directive, in November 2007 the Commission submitted a proposal for a

---


106 Ibid. p. 11.

107 Ibid.
Framework-Decision on the use of the PNR data for law enforcement purposes\textsuperscript{108}. Stating almost the same obligations for air carriers as the Directive 2004/82/EC, namely transmitting the received data to border control authorities of the Member states, the original purpose of the proposal was the fight against terrorist offences and organized crime\textsuperscript{109}.

In contrast to the API Directive the proposal concerns collection and transmission of Passenger Name Records (PNR) instead of API’s. PNR includes around 34 different data elements collected by the travel agencies or the airline companies when a traveler makes a reservation. These data are more detailed and contain, among others all personal data and all forms of payment information. According to the Proposal each Member State must designate an authority, a so-called “Passenger Information Union”, which shall be responsible for collecting, analyzing and transmitting the PNR data which should be kept for a period of 13 years\textsuperscript{110}. The proposal should now be abandoned and replaced by a Council Framework Decision leading to a more comprehensive EU PNR system that should have broader geographic scope and open the possibility to use the data for law enforcement purposes also\textsuperscript{111}.

This proposal raises many concerns in terms of data protection. While the general purpose to fight against terrorism and organized crime is in itself clear, the core of the processing to be put in place does not appear to be sufficiently circumscribed and justified\textsuperscript{112}. This Proposal is contrary to a rational legislative policy in which new instruments must not be adopted before those existing have been fully implemented and proved to be insufficient as well as might otherwise lead to a move towards a total surveillance society\textsuperscript{113}.

Therefore, the proposed measure is not in conformity with fundamental rights, notably Article 8 of the Charter of the Fundamental Rights of the Union, and should not be adopted\textsuperscript{114}.

\textsuperscript{108} Proposal for a Framework Decision on the use of personal Passenger Name Record (PNR) for law enforcement purposes COM(2007) 654.
\textsuperscript{109} BOEHM, supra note 105, p. 13.
\textsuperscript{110} BOEHM, supra note 105, p. 12.
\textsuperscript{111} EU-PNR scheme being re-written by the Council, http://www.statewatch.org/news/2008/oct/04eu-pnr-rewrite.htm (last accessed on 5 November 2009).
\textsuperscript{112} Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (2008/C 110/01), point 25.
\textsuperscript{113} Ibid, point 35.
\textsuperscript{114} Opinion of the EDPS on PNR, supra note 112, point 35.
3.3.2 Private-public-partnership on International level

The public-private-partnership on the International level is exemplified by two cases, the EU-USA Passenger name records (PNR) *case* and SWIFT *case*.

### 3.3.2.1 Passenger Name Record (PNR) case

The public-private-partnership on the International level on the exchange of data is best exemplified by the infamous “PNR” case\(^\text{115}\). In that case were at stake the Commission Decision “on adequate protection” of personal data by the USA authorities and the subsequent Council Decision, which agreed on the transfer of the PNR to the USA authorities. In its short judgment of 30 May 2006 the ECJ found that both the Commission Decision and the subsequent Council Decision should be annulled. ECJ reasoned that these acts do not affect the functioning of the internal market, but their main purpose was to enhance the security and to combat terrorism\(^\text{116}\), and on that ground the court determined that the contested decisions fall outside the common market and as such outside the scope of the Directive 95/46/EC.

From human rights point of view, *this judgment* opened an important gap in the protection of personal data. Instead of placing the judgment within the framework of human rights to privacy (the major substantial issue in the case), the Court was formalistic in its approach limiting itself only to the question of competence\(^\text{117}\). What is surprising is the total absence in the judgment of any reference to human rights protection under International law and binding on the EU Member States, such as the ECHR\(^\text{118}\).

The practical result of such a silence of the ECJ is that the new PNR agreements adopted by the Council in October 2006 and on 23 July 2007 (see Annex II), based on Articles 24 and 38 EU Treaty are even less protective of personal data than the one annulled by the ECJ\(^\text{119}\).

This case will be analyzed further in chapter 4 (section 4.1.2).

---

\(^{115}\) PNR case, *supra* note 21.

\(^{116}\) PNR, *supra* note 21, [2006], at para.55.


\(^{118}\) HATZOPOULOS, “With or without you… judging politically in the field of Area of Freedom, Security and Justice”, (2008), 33 *E.L. Rev.* p.56.

\(^{119}\) HATZOPOULOS, *supra* note 118, p. 57.
3.3.2.2 SWIFT Case

The second case which illustrates the public-private-partnership for collecting and processing data at the International level is *SWIFT case*\(^{120}\). The Brussels-based SWIFT transferred personal banking information to the US government without the knowledge (and the “consent”) of the EU individuals\(^{121}\). The processing of the data by SWIFT\(^{122}\) was in breach of the Data Protection Directive\(^{123}\), nevertheless, showed the quick increase of cooperation between the private and public authorities in the field of data protection.

**As is demonstrated above, cooperation between the private and public authorities both at EU and at International level is increasing quickly.** This development raises many concerns: In addition to the human rights considerations, since they are taking place in the absence of a general data protection framework at the EU level they are being developed without proper consultation of private actors before the implementation of the new measures\(^{124}\). Private actors have to fulfill the conditions imposed by the EU Instruments without having clear rules regulating relation between them and security authorities. EU instruments only state the obligation to store and transmit the data but, regarding the implementation of the imposed measures private actors have to develop appropriate control mechanisms and technical devices on their own\(^{125}\). Recent cases in Germany concerning the misuse of the stored through Germany’s biggest telephone company (Telekom) and a big supermarket company (Lidl) have shown that existing control mechanisms in the private sector are not yet sufficiently developed.

Accordingly, the challenge for the EU legislation is to take measures to provide for robust data protection in the face of such pressure in order to be able to balance privacy needs with security issues\(^{126}\). This is a balancing challenge.

---

\(^{120}\) SWIFT case, *supra note 71*.


\(^{122}\) SWIFT, *supra note 71*.


\(^{124}\) BOEHM, *supra note 105*, p. 12.

\(^{125}\) BOEHM, *supra note 105*, p. 12.

3.4 Information Governance

Contrary to the fears that were at the time of the Directive creation, of centralized control over personal data, users are now also beginning to assume a larger role in managing and reusing their own personal data\textsuperscript{127}. The landscape for the management of the personal data is continually evolving in new ways. The research has demonstrated that the online world is a complicated new environment, where structures that have evolved in the real world over time have to be established in relatively short time\textsuperscript{128}. The main challenge in this respect is the creation of transparency and awareness, as many users are neither aware of the vast quantity of personal data they (voluntary or accidentally) disseminate across the public networks, nor of the potential for reuse or abuse of these data collections\textsuperscript{129}. Therefore, contrary to the assumption of the directive, it has become clear that collection of personal data is not static: their scope, function and ownership can change rapidly and the persons involved are not often aware of how their data may be used\textsuperscript{130}.

3.5 Legal Challenge: construction of a global data protection regime

Given that the privacy is understood differently in the US, Europe and elsewhere, and that the legal category of information privacy (or data protection) is not recognized as such in many countries and given the technological abilities and commercial interests, the question raised is: what should be the global legal regime?

The challenge is not only theoretical, since data flows across the borders, especially in a global economy and a global network. Whereas, previously, trans-border transactions were mostly B2B (Business-to-Business), the new opportunities extend to B2C (Business-to-Consumer), transactions, and thus, immediately raising privacy concerns\textsuperscript{131}.

Local data laws fall short of handling the challenges. Information easily crosses physical barriers and national borders. A data controller who wishes to avoid a local data protection regime could easily set the database and related operations outside that jurisdiction in a “data

\textsuperscript{127} Rand Europe (2008), supra note 52, p.11.
\textsuperscript{128} Rand Europe (2008), supra note 52, p.11.
\textsuperscript{129} KORFF, supra note 98, p.218.
\textsuperscript{130} Explanatory memorandum COM(2007) 698 final, supra note 108, p.12
\textsuperscript{131} RAND EUROPE 2008, supra note 52, p.11.
haven” i.e. country without data protection laws, or less burdensome regulations. Therefore, in order to protect the local data subjects, some sort of mechanisms is required to prevent the circumvention of local data protections.

A complete ban on trans-border data flows would best protect privacy. The opposite choice, abolishing data protection laws, would enable full and uninhibited flows of data across borders to promote free trade and the creation of a global market. The first option would be expensive and unenforceable. Also the second option would threat privacy of the individuals. The answer should be some in between, that is: a data protection (or) privacy regime which empowers the data subjects to decide for herself, if, when, and under which conditions is he/she willing to reveal the data to whom, and for which purposes.

Moreover, although current international instruments such as OECD Guidelines have shown their importance in the world-wide protection of personal data, they are not sufficient as such to safeguard a comprehensive and appropriate personal data protection in the context of digital economy\textsuperscript{132}.

Therefore the privacy legal challenge is to construct a viable global legal regime that would provide data subjects with control over the personal data and at the same time allows trans-border flows. This thesis will attempt to propose in the last chapter, some solutions in order to tackle the legal challenge.

\textsuperscript{132} DUMORTTIER AND GOERMANS, supra note 18.
4 European Data Protection Law: a fragmented legal framework between the First and the Third Pillars

The current European Data protection regime is a complex legal framework, fragmented between the First and the Third Pillars. This fragmentation of the European data protection law under Pillars lines rise many issues.

At the EU level, it raises not only Institutional issue of the choice of Pillars which results in useless “tug-of-war” between EU institutions on where to draw the line between the pillars, but also, the issue of consistency and effectiveness of the EU data protection rules, which results in serious gaps for the European data protection regime. At the International level, the lack of unified data protection regime, as the Passenger Name Records ‘PNR’ case\textsuperscript{133} demonstrates, is an obstacle for the coherence and the unity of the Union’s external action.

The Lisbon Treaty brings about welcome changes for the data protection: it abolishes the Pillar structure of the Union and creates a specific legal basis for the data protection. These changes will address the current problems linked to demarcation of Pillars and pave the way for adopting a general data protection instrument, applicable across different sectors and activities of the EU.

4.1 Inter-pillar demarcation of competence in the field of data protection

Defining the dividing lines between the first and third pillar in the field of data protection is far from easy. The main difficulty arises from the fact that the limitation, stipulated in Article 3(2) of the Directive 95/46/EC\textsuperscript{134}, for issues coming within the Community Law, is not a natural or very practical one, because the boundary between matters within and without the scope of the community law is unclear\textsuperscript{135} and moreover the boundary is continually shifting. A second difficulty is related to the “hybrid” or “twin” acts\textsuperscript{136} covering matters of

\textsuperscript{133} Passenger Name Records, supra note 21.
\textsuperscript{135} KORFF, supra note 98, p. 42..
\textsuperscript{136} HATZOPOULOS, supra note 118, p. 52.
data protection governed by both the First and Third Pillars\textsuperscript{137}. The overlapping of first and third pillar in the field of data protection is unavoidable and these overlaps call for a delimitation of competences.

The relevant criteria for inter-pillar demarcation of competence in the field of data protection derive from the principle laid down in the Article 47 of the TEU (replaced by Article 40 in the treaty of Lisbon) and the relevant case-law of the ECJ.

### 4.1.1 Demarcation of competence between the Pillars: Article 47 EU Treaty

The necessary demarcation between the EC and the EU pillars was governed by Article 47 TEU (replaced by Article 40 of the Lisbon Treaty). This article was not the only provision\textsuperscript{138} which is relevant for the determination of the pillars, but it was the key provision. Article 47 TEU reads as follows:

\textit{“Subject to the provisions amending the Treaty establishing the European Economic Community with a view to establishing the European Community, the Treaty establishing the European Coal and Steel Community and the Treaty establishing the European Atomic Energy Community, and to these final provisions, nothing in this Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them”}.

In accordance with the above mentioned article, nothing in the EU Treaty \textit{“shall affect”} the EC Treaty. The effect of the Article 47 EU Treaty is to render the use of competences in the second and third pillars dependent on the non-existence of competences under the first pillar\textsuperscript{139}. In highly tentative terms, the rather exiguous provision of Article 47 TEU means that, whenever a given measure envisaged by the Union’s Institutions can be taken on the basis of the EC Treaty the measures concerned must not be taken on the basis the EU Treaty\textsuperscript{140}. This overriding principle, laid down in Article 47 TEU, is further elaborated by the ECJ.

\textsuperscript{137} VIS, Euroduc and SIS II, falls partly under the first and partly under the third Pillar.
\textsuperscript{138} Article 1 TEU (Article 1 of the Lisbon Treaty) which presents CFSP and as being supplementary to the European Communities. Articles 2 (Article 2 of the Lisbon Treaty TEU)and 3 (repealed by the Lisbon Treaty) which highlight the maintenance of and the respect for the acquis communautaire, Article 29 of the EU (replaced by Article 67 TFEU) Treaty, which requires maintaining in full the \textit{acquis communautaire}.
The ECJ first came across the relation between the first and third Pillars in *Airport Transit Visa Case*\(^\text{141}\). This case has more than historical value\(^\text{142}\), because clarified the nature of the jurisdiction of the ECJ with regard to the Article 47 TEU. The ECJ rejected the Council argument concerning the Court’s lack of Jurisdiction by grounding its argument on Article 47 of the EU. The ECJ defined its task under Article 47 as being to ensure that EU acts “... do not encroach upon the powers conferred by the EC Treaty on the Community”\(^\text{143}\).

The same matter came before the ECJ in 2003 and 2005, in two cases, concerning respectively the *Criminal Sanctions for the Protection of the Environment*\(^\text{144}\) and *Ship pollution case*\(^\text{145}\).

In the *Criminal Sanctions for the protection of environment* at stake was whether a Framework Decision (2003/80/JHA) which imposed penal sanctions for the protection of the environment had rightly been adopted by the Council within the third Pillar (Articles 29, 31 and 34 EU) and not in the form of a directive under Article 175 EC, on environmental policy. The ECJ ruled that limited harmonization of criminal law may take place in first pillar acts, where this is necessary for the achievement of Treaty objectives\(^\text{146}\).

In the *Ship pollution case* the Commission brought an action for annulment of the Council Framework Decision 2005/667/JHA of 12 July 2005 adopted by the Council (based on Articles 31(1)(e) and 34(2)(b) TEU) to strengthen the criminal-law framework for the enforcement of the law against ship-source pollution. The Commission claimed that the Framework Decision is not the appropriate legal instrument with which to impose on Member States an obligation to criminalize the illicit discharge of polluting substances at sea. The ECJ rules that the aim of the Articles of the Framework Decision was to improve maritime safety, as well as environmental protection and could have been validly adopted on the basis of Article 80(2) EC\(^\text{147}\).

In these cases, ECJ annulled the contested Council Framework Decisions for the same reason: *for encroaching upon the powers of the EC in violation of Article 47 TEU*. In these cases the ECJ interpreted Article 47 TEU broadly, namely, it put very low the *threshold* for a measure to be considered as to adequately contribute to the functioning of the internal market and to trigger the application of Article 47 TEU. This line of case law of broader

---

\(^{141}\)Case 170/96 Commission v Council, (Transit Visa Case), [1998], ECR I-2763.

\(^{142}\)HATZOPHULOS, supra note 118, p. 48.

\(^{143}\)Case 170/96, Transit Visa Case, supra note 141, para.16.

\(^{144}\)Case C-176/03 Commission v Council, [2005], ECR I-7879.

\(^{145}\)Case C-440/05, Commission v Council, [2007], ECR I-9097.

\(^{146}\)Case C-176/03, supra note 144, at para.69.

\(^{147}\)Case C-440/05, supra note 145, para. 69.
interpretation of Article 47 TEU is reaffirmed recently in the *ECOWAS case*\(^{148}\), which related to the relationship between the first and second pillars\(^{149}\).

### 4.1.2 Choice of Pillar in the field of data protection law: ‘PNR’ and Data Retention Directive Cases

The ECJ dealt with the issue of choice of pillar in the field of data protection in two important cases, *Passenger Name Records ‘PNR’ case*\(^{150}\) and *Data Retention case*\(^{151}\).

**The criterion established by ECJ in the infamous ‘PNR’ case is that the purpose of the measure determines the pillar**\(^{152}\). In its short judgment of 30 May 2006 the ECJ found that both the Commission Decision “on adequate protection” of personal data by the USA authorities and the subsequent Council Decision, which agreed on the transfer of the PNR to the USA authorities, should be annulled. The ECJ reasoned that both acts only incidentally affected the functioning of the internal market in air travel services, while the main purpose was to enhance the security and to combat terrorism and other serious crimes\(^{153}\). On that ground the court determined that the contested decisions fall outside the scope of the Directive 95/46/EC.

This *PNR judgment* could not be considered a good law on many accounts. From human rights point of view, this judgment is criticized for opening an important gap in the protection of personal data. Instead of placing the judgment within the framework of human rights to privacy (the major substantial issue in the case), the Court was formalistic in its approach limiting itself only to the question of competence\(^{154}\). What is surprising is the total absence in the judgment of any reference to human rights protection under International law and binding on the EU Member States, such as the ECHR\(^{155}\). The practical result of such an silence of the ECJ is that the new PNR agreement adopted by the Council in October 2006, based on Articles 24 and 38 EU Treaty is even less protective of personal data than the one

---


\(^{149}\) HELISKOSKI, supra note 140.

\(^{150}\) PNR case, supra note 21.


\(^{152}\) DE HERT, PAPAKONSTANTINO and RIEHLE, supra note 96, p. 158.

\(^{153}\) PNR, supra note 21, [2006], at para.55.

\(^{154}\) GILMORE & RIJPMA, supra note 117, pp.1081-1099.

\(^{155}\) HATZOPOULOS, supra note 118, p. 56.
annulled by the ECJ. Therefore the annulment of the contested actions could be described as a Pyrrhic victory for the European Parliament.

The PNR judgment differs from the previous case-law, i.e. Criminal Sanctions for the Protection of the Environment and Ship pollution cases, in which the ECJ has interpreted broadly the scope of Article 47 TEU. The Court’s clear affirmation that the PNR regime falls outside the scope of Directive 95/46/EC, favoured a stricter approach to the scope of community law. The result of this limited approach is that the PNR judgment raised the threshold above which a measure can be considered to contribute adequately to the functioning of the internal market.

Arguably, the audacity of this judgment only served to underline the uncertainty surrounding the delimitation between pillars. The difficulty to apply the PNR judgment in other cases brought before the Court to determine the pillar is clearly illustrated by the Data Retention Case.

The Irish government initiated a procedure before the ECJ to annul the Data Retention Directive on the ground that it falls under the third pillar. The key question raised in this case was (as in the PNR case) the applicability of the community law to the use of personal data collected by private companies for law enforcement purposes. According to the criteria established in the PNR judgment, the activities of the private companies are governed by the First Pillar Data protection rules, but when a legal instrument forces them to process data for enforcement purposes it has to be based on the third pillar Instrument. It is thus difficult to escape the impression that the main objective of Directive 2006/24/EC is that of law enforcement and not the functioning of the internal market. But the ECJ argued that such a line of argument of the PNR case cannot be transposed to the Directive 2006/24/EC and ruled that the Directive comes within the scope of the first pillar. The ECJ reached this conclusion based on the “substantive content” of the measure which according to the ECJ, “relates predominantly to the functioning of the internal market.” ECJ in the Data Retention case, thus, took the view that the substantive content of the measure determine the pillar.

156 HATZOPoulos, supra note 118, p. 57.
157 GILMORE & RIJPMA, supra note 117, p.1081.
158 GILMORE & RIJPMA, supra note 117, p.1095.
160 GILMORE & RIJPMA, supra note 117, p.1096.
161 See the arguments of Ireland in the Data retention Case, supra note 151, at paras. 28-32 and 86.
162 Data Retention Case, supra note 151, [2006], nyr, at para. 90.
163 Data Retention Case, supra note 151, [2006], nyr, at para.93.
164 Data Retention Case, supra note 151, [2006], nyr, at para.85.
The *Data Retention Case* marked again a change in the ECJ approach: The ECJ abandoned the strict approach of the *PNR case*. The result is that ECJ decreased again the threshold above which the measure can contribute to the internal market and thus increased the possibility that a security-based measure falls under the First Pillar.

This wider approach of the Court is also confirmed in *ECOWAS case*\(^{165}\) which concerned the relation between the First and the Second Pillar. The *ECOWAS case* was the first occasion when the Court of Justice is required to draw the line between the EC treaty and Title V of the TEU on the CFSP on the basis of Article 47 TEU. In this case the ECJ annulled a Decision of the Council (2004/833/CFSP) adopted in the framework of CFSP for combating the proliferation of the small arms and light weapons because the subject matter of the Decision falls within the Community Development Cooperation Policy. This is a broad reading of Article 47 EU, based on the *Environmental Crimes*\(^{166}\) and *Maritime Judgment*\(^{167}\) in which the ECJ has upheld the actions brought by the Commission against the acts of Council on the ground that this infringe the Article 47 TEU.

Thus, as the EU law actually stands the choice of pillar in the field of data protection is done following three criteria: **first**, nothing in the EU Treaty “shall affect” the EC Treaty (Article 47 TEU), **second**, the purpose of the measure determine the pillar (‘*PNR* case), and **thirdly**, the substantive content of the measure determine the pillar (*Data Retention Case*).

The question arises as to whether these judgments would still be good law after the entry into force of the Treaty of Lisbon\(^{168}\). Or, would be likely that the ECJ to reconsider (or reverse) its present case-law on Article 47? In the Lisbon Treaty Article 47 TEU is replaced by the new Article 40 TEU which reads as follows:

> “The implementation of the common foreign and security policy shall not affect the application of the procedures and the extent of the powers of the institutions laid down by the Treaties for the exercise of the Union competences referred to in Articles 3 to 6 of the Treaty on the Functioning of the European Union.

Similarly, the implementation of the policies listed in those Articles shall not affect the application of the procedures and the extent of the powers of the institutions laid down by the Treaties for the exercise of the Union competences under this Chapter.”

---

\(^{165}\) *ECOWAS case*, supra note 148.

\(^{166}\) Case C-176/03, supra note 144.

\(^{167}\) Case C-440/05, supra note 145.

\(^{168}\) Lisbon Treaty entered into force on 1 December 2009.
This new article differs from the current Article 47 TEU in two important ways. The first and the most obvious change is that, the new Article 40 TEU would govern the relationship between the exercises of the Union competence under the CFSP on the one hand and under all other policies or activities of the Union on the other hand, that is non-CFSP competence. In the Treaty of Lisbon, the current Title VI TEU (Police and Judicial Cooperation in Criminal matters) would cease to exist as a separate “Third Pillar” and the activities concerned would become subject to the general legal framework of the Treaty on the Treaty on the Functioning of the European Union\textsuperscript{169}. Consistent with that change the Union will act by means of the instruments that have hitherto only been available to the Community\textsuperscript{170}. In such a situation there would no longer be a need for a provision such as the current Article 47 TEU to governs the relationship between those and other activities of the Union\textsuperscript{171}. The only issue that can be raised is the choice of legal basis of measures of “Third Pillar” and “First Pillars”. But the case law delivered by the ECJ under the EC Treaty concerning the choice of legal basis for a measure with several objectives or components is well-settled\textsuperscript{172}. The ECJ applies the “centre of gravity” theory\textsuperscript{173}, namely, in situations where a measure covers areas falling under the different legal bases the act must be based on the legal basis required by the main or predominant purpose or component.

In the light of the wording of the new Article 40 TEU, the second change is that, this Article clearly gives “equal weight” to competence deriving from the CFSP and Non-CFSP legal bases: the implementation of the CFSP shall not affect the application of the procedures and the extent of the powers of the institutions laid down by the Treaties for the exercise of the Union competences and vice versa\textsuperscript{174}. Interpreted in this way the new provision of Article 40 TEU would no longer give primacy to the exercise of the Non-CFSP competence over the CFSP competence (the current approach). Therefore the rationale of the provision would rather be to prevent any interference between the two categories of procedures and powers.

Finally, while the above mentioned problems concerning the “choice of Pillars” between the Community Pillar and the Third Pillar will disappear, the problems of concerning the choice of pillars between the CFSP and non-CFSP issues are not likely to disappear—quite to contrary\textsuperscript{175}.

\begin{footnotesize}
\textsuperscript{169} See chapters 4 and 5 of the Title V of the Part 3 of the Treaty on the Functioning of the European Union.
\textsuperscript{170} TFEU Art.288.
\textsuperscript{171} HELISKOSKI, supra note 140, p. 910.
\textsuperscript{172} HELISKOSKI, supra note 140, p. 906.
\textsuperscript{173} GILMORE & RIPMA, supra note 117, p.1092.
\textsuperscript{174} HELISKOSKI, supra note 140, p.911.
\textsuperscript{175} HELISKOSKI, supra note 140, p. 912.
\end{footnotesize}
4.2 Data Protection Law in the First Pillar

In the framework of the First Pillar the data protection is ensured by the Data Protection Directive 95/46/EC (considered as *lex generalis*) and other sectoral directives (*lex specialis*), which detail the rules and principles laid down in the Directive 95/46/EC. While the protection of the personal data by the Community institutions is governed by the Regulation (EC) No. 45/2001.

So far, the Directive 95/46/EC is credited both for reforming the data protection law of the EU Member States, and for becoming a global good practice of data protection law to be followed by other countries and regions outside Europe. However, the Directive has many weaknesses which call for its review in order to meet the new challenges posed to privacy and to keep its so far global influence.

### 4.2.1 Data Protection Directive 95/46/EC

Directive 95/46/EC is the reference legal instrument for data protection at the EC level. The Directive was adopted on 24 October 1995 to regulate the processing of *personal data*, prescribing how and under which circumstances personal data can be processed. As the title shows, the Directive is based upon two pillars. The first pillar concerns the protection of natural persons with regard to the processing of personal data (Article 1(1)), and the second one concerns the free movement of such data (Article 1(2)). The content of the Directive is often expressed in terms of six main principles (Article 6), (*legitimacy, purpose-limitation, transparency, proportionality, confidentiality and security, and control*) which are its heart and underline it.

These principles specified in the case-law of the ECJ concerning the interpretation of the Directive, taking into account particularly the principle of proportionality and the respect

---

176 Directive 95/46/EC, supra note 134.
177 Council Regulation (EC) No 45/2001, of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, O.J. L. 8, 12.1.2001.
of fundamental rights as enshrined in the Article 6 TEU as well as in Article 8 of the European Convention on Human Rights.\(^{179}\)

The directive applies to any automated processing of personal data and any other handling of personal data that forms part of a filing system (Article 3(1)). However, the Directive does not apply to processing operations concerning the activities (public security, defence), which fall outside the scope of community law, (Article 3(2)).

The CJEC has ruled on the Data Protection Directive in four instances that national courts conferred with questions on the interpretation of EC law. First, in an Austrian case Rechnungshf\(^{180}\), the CJEC held that the processing of personal data within the public sector is covered by the Data Protection Directive. The plaintiff can invoke specific provisions of the directive that grant individual rights before national courts if the national data protection law contradicts these rights. Second, in another case from Sweden (Bodil Lindqvist\(^{181}\), the CJEC decided that the main principles of the directive also apply to Web sites, and that the uploading of personal information for Internet access does not trigger the provision for transfers of personal data to third countries even though the Web page is universally accessible.

The two last cases are very recent of December 2008 Huber case\(^{182}\) and Satamedia Oy case\(^{183}\), both Judgments delivered on 16\(^{th}\) December 2008. In Huber case, a German case, the ECJ made an interpretation of the concept of necessity under Article 7(e) of the general Data Protection Directive. The ECJ held that a system for storage and processing of personal data relating to Union citizens who are not nationals of the Member State concerned, does not satisfy the requirement of necessity laid down by Article 7(e) of Directive 95/46/EC, interpreted, in the light of the prohibition on any discrimination on grounds of nationality. The Satamedia Oy case, a finish case, raised some interesting questions: first, whether activities, such as collected from documents in the public domain held by the tax authorities and processed for publication for commercial purposes, fall within the scope of the directive and can be regarded as processing of personal data under its Article 3(1), second, the interplay between the personal data and the freedom of expression (Article 9), that is, whether above various activities can be regarded as the processing of personal data carried

---

179 FRANZISKA, supra note, 15, p. 3.
181 Case C-101/01, Criminal Proceedings against Bodil Lindqvist, [2003], ECR I-12971.
182 Case C-524/06, Heinz Huber v Bundesrepublik Deutschland [2008], Judgment of 16 December 2008, not yet reported.
183 Case C-73/07, Tietosuojavaltuutettu v Satamedia Oy, Judgment of 16 December 2008, not yet reported.
out ‘solely for journalistic purposes’ within the meaning of Article 9 of the Directive. The ECJ held that, first, activities such the collection of personal data from tax authorities and published for commercial purposes fall within the scope of the directive and are processing of personal data under Article 3(1) of the Directive and second, such activities must be considered as activities involving the processing of personal data carried out ‘solely for journalistic purposes’ under the Article 9 of the Directive, therefore exempted from general principles of the Directive. These cases will be put into discussion when and where relevant.

From 1995 the Directive caused a wave of reform both within the EU Member States and at the Global level. Due to the Directive, at the EU level, the differences between the legal provisions of the Member States were reduced, at the global level the Directive is credited for becoming a unique form of soft legal globalization184. The data protection laws of other countries (Israel, Japan etc.) and regions (Americas, Asia) are modeled after the EU Directive, which is acknowledged as the main engine of an emerging global legal regime on data protection, (See Annex I).

However, over time due to the technological developments basic assumptions of the Directive have been challenged and this questions both its ability to fit the objectives for which was adopted in 1995 and to retain its thus far global influence.

### 4.2.2 Regulation (EC) No. 45/2001 on the protection of personal data by Community Institutions

Although Directive 95/46/EC provided for comprehensive principles of data protection at the European Community level, it only applied to MS, since only MS can be addressed by a directive (ex Article 249 paragraph 3 of the EC Treaty, now Article 288 TFEU). In consequence the Directive did not cover the processing of Data by organs of the EU Community. To solve this problem, the treaty of Amsterdam in 1999 introduced Article 286, (replaced by Article 16 of the TFEU). This Article extended the application of data protection principles also to personal data processed by European Community institutions and bodies set up by or on the basis of the Treaty. In addition Article 286 paragraph 2 obliged the Council to establish an independent supervisory body responsible for monitoring the application of such community acts by community institutions and bodies.

---

184 BIRNHACK, supra note 5.
In this perspective, detailed provisions based on this article were laid down by Regulation 45/2001 which also established a supervisory authority at Community level, the European Data Protection Supervisor. However, like the Directive 95/45/EC the regulation does not apply to activities falling completely within the activities of the third pillar nor does its provisions apply to bodies fully established outside the community framework.

The CFI has subsequently clarified the scope of Regulation in two cases. The first case Bavarian Langer case concerns the interplay between the Right to public Access to EU Documents and the Data Protection Rules and the second, the case Nikolaou, and the violation by the EC Institutions (OLAF) of the Regulation no. 45/2001.

In the Bavarian Langer case the Court clarified the relationship between the Regulation (EC) No.1049/2001 regarding public access to the EU Institutions documents and the Regulation No.45/2001 on data protection by the EU Institutions. While the Court acknowledged that professional activities could fall under the concept of private life, as protected by Article 8 of the ECHR, on the other hand held that “not all personal data are capable by their nature of undermining the private life of the persons concerned”. The CFI concluded that, the full minutes of the meeting, containing all the names of the participants, does not fall within the exceptions under Article 4(1) of Regulation no. 1049/2001, and that the persons concerned by the disclosure of the personal data had no right to object the disclosure as foreseen by the Regulation No. 45/2001. Therefore, the CFI annulled the Commission decision of 18 March 2004, which rejected the applicant request for access to the full minutes of the meeting of 11 October 1996, containing the names of all participants.

The case Nikolaou, the TFI condemned the European Commission (even though with a symbolic financial penalty), for moral damage caused by OLAF (European Anti Fraud Office) to Mrs. Nikolaou (former member of the Audit Court of the European Communities). The CFI held that the information, given by OLAF officers to European Voice (A newspaper Covering EU Issues), concerning the investigations pursued by OLAF against Mrs. Nikolaou, constituted violation of the data protection rules laid down in Regulation No. 45/2001.

---

4.2.3 Directive 2002/58/EC on privacy and electronic communications (E-privacy Directive)

The EC took specific measures to ensure the protection of privacy in the field of telecommunications. First, in 1997 with the Telecommunications Privacy Directive (1997/66/EC), which is no longer in force and then, in 2002, with the Directive on Privacy and Electronic Communications.

The Directive 2002/58/EC was adopted by the EU in order to fill the legal lacuna of Article 25 and 26 of the Directive 95/46/EC. As the “Echelon Case” demonstrated certain situations could not fall easily under the application of the so-called transborder data flows (TBDF) provisions (Articles 25 and 26) of the Directive 95/46/EC, in so far as they are not the consequences of directly or indirectly voluntary transmission by a person located in Europe\(^{188}\).

In the “Echelon Case” due to the characteristics of the communications by satellite, the US and the UK governments have developed a system of electronic surveillance able to read the communications passing through this way of communication including a communication sent by a person located within Europe and having as receiver another EU citizen. In that case, the transmission outside of Europe is the result of the global and interactive nature of the networks, used by the EU residents and there was no transfer in the sense of the Directive 95/46/EC. It was thus possible to the UK (as well as Canada, Australia and New Zealand) and the US intelligence services to spy every European citizens, companies or administrations whose communications were circulating satellites without trespassing the EU borders\(^{189}\).

The EU Parliament six days before the 11\(^{th}\) September has strongly reacted to these new privacy threats and to this violation of its sovereignty by claiming the adoption by the EU of new tools in order to better ensure its citizens privacy and its sovereignty\(^{190}\).

This situation leads EU to enact in 2002, a specific Directive as regards “Data Protection and the Electronic Communications Sector” in order to face these new threats.

\(^{188}\) POULLET, *supra note 41*, p. p.5.

\(^{189}\) *Ibid.*

\(^{190}\) European Parliament resolution of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)).

In that respect, the provisions of the 2002/58/Directive regulate certain activities of data controllers, notwithstanding the fact that they are located inside or outside of Europe. The activities like economic communication interceptions, use of traffic or location data, sending of unsolicited communications are under the EU regulations, even if they are operated from outside Europe.

Therefore, provisions of the Directive 2002/58/EC target all the electronic communication services without taking into account the nationality or the establishment of their providers. In that sense, one might speak clearly about the extraterritoriality of this Directive\textsuperscript{192}. This will be discussed further in the last chapter (section 8.4.2).

The main challenge that this directive is facing is to keep pace with the new technological developments, or otherwise their Articles will become obsolete. In 2007 the Commission proposed amendments to the e-Directive\textsuperscript{193}, which does not reshape entirely the existing measure, but rather, propose ad hoc amendments which aim at strengthening the security related provisions (Article 4), improving the enforcement mechanisms (Articles 13 and 15) as well as modernizing certain provisions that have been outdated (Articles 2(e), 3(1), 5(3))\textsuperscript{194}.

On the whole the proposal is welcome, however it fail to address one of the most worrisome issues of the e-Privacy Directive, namely, the problem of the scope of its application (Article 3) which is currently limited to the public electronic communication networks (Article 3)\textsuperscript{195}. EDPS argues that, the scope of application of the e-Privacy Directive should be broadened to include the electronic communications provided by the private and mixed (private/public) networks\textsuperscript{196}. To broaden its scope is necessary, because the services are increasingly

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{192} POULETT, \textit{Y}. supra note 41, p. 12.
\item \textsuperscript{194} Commission Proposal, supra note 193, p.6.
\item \textsuperscript{196} EDPS Opinion 2008/C 181 /01, see supra note 195, point 68.
\end{enumerate}
\end{footnotesize}
becoming a mixture of private and public elements and therefore, it is often difficult for regulators and for stakeholders alike to determine whether the e-Privacy Directive applies in a given situation. Furthermore, in dealing with the new issues such as the setting up of a mandatory breach of notification system (Article 4), the proposal only offers partial solutions, not including within the scope of the organizations obliged to notify security breaches, entities that process very sensitive types of data such as the on-line banks, or the providers of on-line health services. This critique of the EDPS is also endorsed by Article 29 Data Protection Working Party in its opinion 2/98 on the e-Privacy Directive.

4.2.4 Data Retention Directive: a controversial measure

Data Retention Directive 2006/24/EC, adopted in 2006, provides for the obligation of the Member States to require from the communication providers to retain communication data (Article 3) for a period of between 6 months and 2 years (Article 6). This Directive applies only to communication data, necessary to identify subscribers or user, and excludes from its scope the retention of data revealing the content of communications (Article 5(2)). The providers must retain all data concerning phone-calls, faxes, e-mails, internet use and mobile phone calls of their clients, including names, addresses, dates, time and destination of communication.

While the main reason for the adoption of this Directive, i.e. to combat terrorism and organized crime, sounds justified, its adoption has raised many concerns and has been subject of harsh criticisms from many perspectives.

From a procedural perspective, the proposal of the Directive was largely prepared in secret by the Council and was adopted hastily (by accelerated procedure). The Council exerted

---


198 EDPS Opinion 2008/C 181 /01, supra note 195, p.3.


200 Directive 2006/24/EC, supra note 103.

201 DE HERT, PAPAKONSTANTINO and RIEHLE, supra note 96, p. 156.
pressure on the European Parliament to vote the Directive and in exchange promised the adoption of the Framework Decision on data protection in the third Pillar.\footnote{DE HERT, PAPAKONSTANTINOU and C. RIEHLE, supra note 96, p. 163.}

From a substantial point of view, the Directive creates considerable legal gaps and uncertainty for the data protection law. Firstly, the Directive allow the Member States to decide to keep the data, longer term than the maximum period of two years, if they find necessary (Article 12), which lead to a Polish law allowing mandatory telephonic data retention for 15 years.\footnote{DE HERT, PAPAKONSTANTINOU and RIEHLE, supra note 96, p. 157.} Second and most notably, the Directive requires indiscriminate collection and retention of data on a wide range of European activities, whereas traditional police work only target suspected persons. There has never been a policy mandating the storage of information based on the possibility that it might be of interest at some points in the future.\footnote{Ibid. p.157.} In this respect, the WP29 pointed out that the Data Retention Directive "...is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish."\footnote{WP29 Opinion 3/2006 on the Council Directive 2006/24/EC, p. 2, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf}

Thirdly, the mandatory data retention for the sake of law enforcement, challenges at least two important principles of data protection law, the principle of proportionality, i.e. that the communication service providers should not retain their data for longer periods than required for business purposes, and the principle of purpose limitations, i.e. that the subsequent use of data should not be allowed for purposes not contemplated at the time of collection.

Furthermore the lack of competence, the necessity and the proportionality of the Directive were also criticized by the Data Protection Authorities.\footnote{BOEHM, supra note 105, p. 10.}

In addition, service providers wonder how they are supposed to cover the high implementation costs, which are necessary to expand their storage space and to guarantee the security of the stored data.\footnote{BOEHM, supra note 105, p. 11.}

Therefore, the adoption of this Directive has caused protests by the civil society organizations in many EU countries (e.g., Germany and Sweden) and actions both against the Directive itself (Data Retention Case)\footnote{Case C-301/06, Ireland v Parliament and the Council, supra note 151.} and against the national laws transposing the data retention directive. In April 2008, 43 civil liberties NGOs and professional associations...
signed a submission claiming that data retention violates the right to respect of the private life and correspondence, freedom of expression and the right of providers to the protection of their property\textsuperscript{209}. They urged the ECJ to base its decision on the incompatibility with human rights rather than lack of competences.

Moreover, there has been reaction from the Member State themselves. Romanian Government, in a sudden move has decided on 25 February 2009 to suspend the application of the data retention law until the end of the year (2009).

4.2.5 Additional Data Protection-related Instruments in the First Pillar

Besides the EU Data Protection Directive 95/46/EC there are a number of other European Directives which may also contain the data protection rules relevant to the specific sector or categories of data. For example the Directive on the re-use of the public sector information\textsuperscript{210}, Distance Selling Directive for the protection of consumers\textsuperscript{211}, E-Commerce Directive\textsuperscript{212} and the Electronic Signature Directive\textsuperscript{213}.

Besides, Directive, other instruments in the framework of the First pillar are Recommendations and Opinions, such as those of the Article 29 Working Party. They are not binding in a strict legal sense, but can be persuasive as an indication of the likely present state of law.

\textsuperscript{209} BOEHM, supra note 105, p.11.


4.3 Data Protection in the Second Pillar (CFSP): no harmonized standard governing data protection

As far as the Common Foreign and Security Policy (CFSP) is concerned, there is no harmonized standard or general framework governing data protection. However, the European Courts have established case-law on the legitimacy of some activities of the CFSP regarding the management of the so-called terrorist blacklist, lists of individuals and organizations whose assets are frozen because of their presumed connection with terrorist organizations, on the basis of information originating either from the United Nations or from the Member States. In the cases Sison v Council and Organization des Modjahedines de People d’Iran (OMPI) v Council, the TFI has annulled some of these listings on the basis of the lack of compliance with the basic procedural rights, such as the right to be informed about the reasons for inclusion in the list or the right to an independent review of the decision. The applicants achieved their erasure from the blacklist and consequently, in April 2007 the Council agreed to a new policy regarding the way in which individuals and groups are added to the list, taking into account the OMPI case. According to the new policy the Member States are required to provide information concerning the reasons for the placement of the persons on the list. However, this development requires data exchanges between private actors (i.e. banks), National security authorities and EU institutions leading to cross-pillar data flows without a legal framework for these measures.

The Lisbon Treaty extends the data protection to the CFSP. Article 16 of the TFEU lays down the legal basis for one comprehensive legal framework applicable across different activities of the Union, including CFSP. However, the extension of the scope of the data protection rules to the CFSP should carefully take into account the specific provisions laid down by the new article 39 of the Union Treaty. Article 39 of the Union Treaty derogates from the paragraph 2 of the Article 16 TFEU, by establishing that specific rules on the protection of personal data processed by Member States in the area of the CFSP will be laid

---

215 FRANZISKA, supra note 15.
216 SCIROCO, supra note 214.
219 SCIROCO, A., supra note 214.
220 FRANZISKA, supra note 15, p. 4.
221 FRANZISKA, supra note 15.
222 SCIROCO, A., supra note 215.
down by the Council and that also in this case their application shall be subject to the control of independent authorities.\textsuperscript{223}

The subjective right to the protection of the personal data laid down by Article 16, paragraph 1, will still apply in this area, but the procedure for the adoption of the specific rules will not involve the European Parliament. However, since Article 39 establishes derogations only with regard to processing of personal data by Member States, the general provision of Article 16 seems to remain fully applicable - including the involvement of the European Parliament- in the case of processing of personal data by European Union Institutions.\textsuperscript{224}

4.4 Data Protection Law in the Third Pillar: weak and not productive

All police and judicial databases on persons can be considered sensitive in themselves, whether their use violates the privacy or not. Accordingly, strict control is necessary to avoid the infringement of the right to privacy and data protection by security policies. The urgency of this necessity is heightened when police forces start exchanging their own data with foreign colleagues or supranational bodies such as Europol.

The data protection law in the Third Pillar is governed by the Framework Decision\textsuperscript{225} for the protection of the personal data in the Third Pillar (considered as lex generalis) and other specific data protection rules (lex specialis)\textsuperscript{226} incorporated in various legal instruments of the Third Pillar.

4.4.1 Specific data protection provisions

The exchange of personal data within the current EU’s police and Judicial cooperation network takes place between different actors. On the one hand, there are the Member States and the EU Institutions and on the other hand, private actors and the third parties (states or International Organizations). This constellation leads to four different exchange

\textsuperscript{223} SCIROCO, supra note 214.
\textsuperscript{224} SCIROCO, supra note 214.
\textsuperscript{225} Council Framework Decision 2008/977/JHA, supra note 243.
possibilities. Firstly, reciprocal data transfer between the Member States and the EU institutions in the framework of centralized data bases. Secondly, exchange between the Member States and private actors (public/private partnership in combating crime, such as the Data Retention Directive, API Directive and EU-PNR). The third possibility is the transfer of data between private actors and third parties (PNR and SWIFT cases). The forth possibility concerns the direct exchange of information between the Member States themselves, based on intergovernmental agreement in the context of decentralized databases, i.e. outside the EU’s framework.

Each of these different data exchange possibilities implies their own problems and strict control is necessary to avoid the infringement of the right to privacy and data protection by security policies.

Arguably, there are serious objections to the various instruments put at place in the Third Pillar to enhance the exchange of data between EU Member States and (more worryingly) with third states. For instance, Schengen Information System (SIS), since its implementation in 1995, more than 22 million records have been created and the amount of registered data is increasing quickly. These initiatives, notably the principle of interoperability and the principle of availability, undermine the data protection principle of purpose-limitation, requiring data to be collected only for a specific purpose and not to be used for any other purpose. Moreover, the ever-expanding scope of Europol to almost all sorts of crimes without proportional measures and safeguards for the protection of human rights creates tension with human rights principle of proportionality. Therefore, these developments demand a clear data protection framework.

227 FRANZISKA, supra note 15.
228 I.e. the data bases of Europol, Eurojust, Schengen Information system (SIS) and Custom Information System (CIS).
231 The Treaty of Prüm was signed on 27 May 2005 by the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria, Council Document 10900/05, 7 July 2005.
232 FRANZISKA, supra note 15.
233 Communication from the Commission on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM (2005), 597 final, 24 November 2005.
235 DE HERT, PAPAKONSTANTINOU and RIEHLE, supra note 96, p.153.
Since Directive 95/46/EC does not apply to the Third Pillar, the legal instruments on Schengen, Eurojust, Europol, CIS and Prüm Framework had foreseen specific data protection rules resulting in a fragmented body of provisions. Common to all these systems are three legal sources which should assure compliance with data protection rules in this area: Firstly, individual data protection rules stemming from the legal instruments of the organization themselves, secondly, principles coming from the Council of Europe Convention No. 108 and thirdly, rules of the Recommendation of the Committee of the Ministers of the Council of Europe regulating the use of personal data in the police sector (R(87) 15). The individual data protection rules of the above mentioned instruments (i.e. Europol, Eurojust and CIS Conventions, and the Convention implementing the Schengen Agreement), which are first of all, applicable in cases of misuse, state their own specific data system, but refer to Council of Europe Convention No. 108 and to the recommendation R (87) 15 regarding their data protection standard. This means, if individual instruments of the organizations do not cover the circumstances of a particular case, the rules of the Council of Europe Convention No. 108 apply.

However, these instruments cause serious confusion and difficulties for the data protection. These instruments are not data protection instrument in themselves, on the contrary, they facilitate the data exchange between the law enforcement bodies and thus contribute to the erosion of principles of privacy and data protection.

Another difficulty is that both Convention No. 108 and Recommendation R (87) 15, contains general rules and principles rather than detailed regulation, which leaves most to the discretion of the Member States. Additionally, Convention and regulation are legal mechanisms of the 1980s and have never been substantially renewed since this period.

Therefore, the data protection rules as well as the legal sources of the different centralized data bases of the third pillar very a lot. On the one hand, very specialized data protection rules of the organizations (Europol, Eurojust, SIS and CIS) and on the other, generally

---

236 See the relevant articles, supra note 226.
238 FRANZISKA, supra note 15.
239 FRANZISKA, supra note 15.
240 FRANZISKA, supra note 15. The Council of Europe Convention No. 108 was amended in 1999. Member States agreed to apply the convention also to information relating to groups of persons, associations, foundations, companies, corporations and any other body consisting directly or indirectly of individuals, whether or not such bodies possess legal personality. They also agreed to apply this Convention to personal data files which are not processed automatically.
oriented legal instruments which have not been renewed since the 1980s (Convention No. 108 and Recommendation R (87) 15).

These statutes do not provide a clear protection framework which responds to the challenges of the current security requirements as they were developed in a different context almost 30 years ago\textsuperscript{241}. Thus the deficit of the general rules adapted to current security challenges caused concern. Fully aware of these risks and tensions the Commission in 2005 proposed a Council Framework Decision\textsuperscript{242} for data protection in the Third Pillar, to which we now turn.

\subsection*{4.4.2 Framework Decision 2008/977/JHA: a “police cooperation” document or a “data protection” text?}

The EU adopted the \textbf{Framework Decision on the protection of personal data in the third pillar}\textsuperscript{243} in November 2008, after three years from the submission of the Commission proposal. This measure is the first horizontal measure adopted to ensure a coherent framework of data protection in the third pillar.

Its main purpose is the establishment of a common level of data protection which applies to cross-border exchanges of personal data within the framework of police and judicial cooperation. The Framework Decision contains rules applicable to onward transfers of personal data to third countries and to the transmission to private parties in Member States. The framework decision as a horizontal act of data protection does not affect the relevant set of data protection provisions of several acts adopted pursuant to the Title VI of the TEU before the framework decision, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States because they regulate the matters in more detailed than the framework decision.

The adoption of this Framework Decision appears necessary, given the existence of only case-specific legislation of several acts in the third Pillar (i.e. Schengen, Europol, Eurojust and CIS) adopted, before the Framework Decision. This set of specific data protection

\footnotesize{\begin{itemize}
\item \textsuperscript{241} FRANZISKA, supra note 15, p. 9.
\item \textsuperscript{243} Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J.L.350.
\end{itemize}}
provisions, need to be based on a general legal text, a text that ought to have preceded them, but which is, nevertheless, welcome \(^\text{244}\).

However, the expectations were to adopt a solid instrument of data protection consistent with the principles laid down in the Directive 95/46/EC. In fact this was the approach proposed by the European Commission in 2005. Both the structure of the proposed Framework Decision (except for Chapter III-specific types of processing which was entirely unprecedented) and the approach to the subject-matter were drafted along the lines of the Directive 95/46/EC \(^\text{245}\).

But, the original proposal of the Commission was amended and the final text of the Framework Decision adopted by the Council in 2008 looks more like a ‘police cooperation’ document, than a ‘data protection’ text. Moreover, it is questionable whether for certain aspects the Framework decision provides for the same level of protection as defined in Council of Europe Convention 108. This seems to be the case with the provisions on the further use of data received from another Member State (Articles 3 and 11) and the right of access (Article 17) \(^\text{246}\).

Accordingly, the Framework Decision has been subject to much criticism from various stakeholders (European Parliament and EDPS) and academics. There are many aspects of the Framework Decision to be criticized, but, the most important concerns are the following:

First, the Framework Decision excludes from its scope the Member State domestic data (Article 1). The Framework Decision only covers the police and judicial data exchanged between EU Member States, EU authorities and systems. Moreover, the Framework Decision does not apply to the police and intelligence activities in the field of national security.

Second, the Framework Decision does not distinguish between different categories of data subjects, such as suspects, criminals, witnesses and victims, to ensure that their data are processed with more appropriate safeguards \(^\text{247}\).

Third, the Framework Decision does not ensure an adequate level of protection for exchanges with third countries according to a common EU standard (Article 13) \(^\text{248}\).

\(^{244}\) DE HERT, PAPAKONSTANTINOU and RIEHLE, supra note 96, p. 179.

\(^{245}\) Ibid. p.165.


Forth, does not provide consistency with the first pillar’s Data protection Directive 95/46/EC, in particular by limiting the purposes for which personal data may be further processed\(^\text{249}\).

All these problems makes the new Framework Decision such a weak legal instrument that it will be a surprise if it will succeed “in guarantying a more harmonized set of regulation and strengthen the civil liberties in Europe”\(^\text{250}\). The weaknesses of the Framework Decision clearly show the lack of a common data protection standard in the current third pillar matters. Therefore, the EDPS recently recommended to include in the Stockholm-programme, as a priority, the need for a new legislative framework, \textit{inter alia} replacing Council Framework Decision 2008/977/JHA\(^\text{251}\).

\section*{4.5 Changes in the Lisbon Treaty: New horizons for the data protection in the European Union?}

The Lisbon Treaty, which entered into force on 1 November 2009\(^\text{252}\) brings about welcomed changes not only to the future of the European Union, but also to the right for data protection. The Treaty put to an end the pillar structure of the EU, Article 16 of the TFEU explicitly provides for the right to data protection and the Charter of the Fundamental Rights of the Union\(^\text{253}\), which includes in Article 8 a provision on data protection become a binding instrument.

Article 16 of the TFEU is of crucial importance for the data protection in many perspectives and there are many aspects to be welcomed in this new provision. Most importantly, a subjective right to the protection of personal data (Article 16(1)) and the “constitutional” need for rules in data protection is enshrined in the EU primary law (Article 16(2))\(^\text{254}\).

\begin{footnotesize}
\begin{enumerate}
\item EDPS, supra note 247.
\item Ibid.
\item DE HERT, PAPAKONSTANTINOU and RIEHLE, supra note 96, p. 122.
\item OJ. C. 115/1 of 9.5.2008.
\item OJ C 303 of 14.12.2007, p.1
\item SCIROCO, supra note 214.
\end{enumerate}
\end{footnotesize}
The creation of a self-standing legal basis for the Union to legislate in this matter, combined with the “normalization” of the decision-making process, i.e., the possibility to adopt these rules through the “ordinary legislative procedure” and the abolition of the Pillar structure of the Union paves the way for adopting a comprehensive legal instrument for data protection, applicable across different activities of the Union. A comprehensive data protection framework would enhance the consistency of the system, ensures legal certainty and by doing so improves the protection. In particular, it would avoid in the future the difficulties of finding a dividing line between the pillars255.

In addition, the Treaty of Lisbon brings another important improvement relevant for the data protection: it grants the Union the competence (and the obligation) to accede to the European Convention of Human Rights (Article 6(2)) and confirms that fundamental rights as guaranteed by the ECHR shall constitute general principles of the EU law (Article 6(3).

These novelties are very important and add substance to the protection of personal data. The Charter of the Fundamental Rights of the EU provides for the right to data protection in Article 8. The merit of this article is that it spells out the essential elements of data protection right, requiring that the personal data need to be processed “fairly”, for “specified purposes”, and based on “consent” as well the right of the data subjects to “access” and to “rectify” their data.

Also the “double tie” of the Union with the ECHR is particularly important because it confirms the relevance of Article 8 ECHR and the case-law256 of the Strasbourg Court within the EU legal framework257. This means that the EU and its Institutions will be accountable to the Strasbourg Court for the issues concerning the ECHR258.

On the one hand, the Lisbon Treaty marks an important and visible consolidation in the European Union primary law of the data protection acquis developed in Europe over the last 27 years259. In this perspective, the Lisbon Treaty pinpoints some crucial elements of the fundamental right to the protection of personal data, within the context of the increased protection of fundamental rights.

256 See the ECtHR case-law of Article 8 of ECHR (right to privacy): Case Rotarou v. Romania, Judgement of 4 May 1999; Case Tyrer v. UK, Judgement of 25 April 1978; Case Selmouni v France, Judgement of 28 July 1999; Case Matthew v. UK, Judgement of 18 February 1999.
257 SCIROCO, supra note 214.
259 SCIROCO, supra note 214.
On the other hand, it develops instruments for a stronger and more homogeneous data protection across the different activities of the European Union. In this perspective the new tools laid down in the Lisbon Treaty represent a challenge for the European Data Protection Law in the 21st century. The first challenge is related to the efforts required to address the new threats posed to privacy, namely, the growing demand for security and the immense possibilities offered by new privacy-destroying technologies. A second equally important challenge, for the EU Data protection law is to build on the so far global influence as a good practice for the data protection, which means to become a preferred model of the privacy understanding at the global level, prevailing over other competing models, notably the US privacy model. To meet these challenges many horizons are possible.

However, what is required as a first step is to review the current legal framework of the EU, notably the Directive 95/46/EC and to build a data protection legal framework which is comprehensive and general, but at the same time able to accommodate the specificities of certain areas.
This chapter explains briefly the essential legal concepts of the directive, that is, the objectives and the principles of the directive, the data subject rights, controller's obligations and the export of the data to third countries.

### 5.1 Conflicting Objectives

The Directive aims to serve two conflicting objectives: first, protecting the “fundamental rights and freedoms of natural persons in particular their right to privacy with respect to the processing of the personal data” (Article 1(1)) and second, allowing the “free flow of personal data between the Member states” (Article 1(2)).

Instead of presenting “privacy” and “free flow of personal data” as conflicting, the directive ties them together. Tying together two conflicting interests, managed to avoid the very real conflict between the two goals, but was exposed too much criticism. Gutwirth offers sharp criticism: “everything the Commission touches becomes a market”\(^{260}\). The goal of achieving an internal market was elevated, he argues to the same level of fundamental human rights and more so, “The concern about the privacy is totally subordinate to the market prerogatives”.

This criticism of Gutwirth is grounded because, initially the proposal for the directive was generated by human rights concerns, but the Commission proposed the directive as a single market harmonization issue. In its background document concerning the Data Protection Directive, the Commission has explained that “the raison d'être of the Directive is the Single Market”\(^{261}\) and not the human rights.

This is at odds with the raison d'être of any data protection law which, as we analyzed above, is the legal reaction to the threats posed to the privacy by the mass processing of information relating to individuals. It is true that there is an inherent conflict between the protection of the data and the free flow of personal data. It is also true that the task of balancing these two opposing interests is delicate and unlikely to be accomplished once and

\(^{260}\) BIRNHACK, supra note 5, p.8.

for all. But, since their conflict is inherent the emphasis may be placed on one or the other. What is wrong in the Directive approach is that, while the emphasis should be put on one or the other of these inherently conflicting interest, the Directive either tie them together, or even worse gives priority to market interests. This approach is at odds with the *raison d’être* of the data protection laws, analyzed above. Therefore what is needed in principle, in the framework of the review of the directive is the need to shift from this market approach towards the emphasis on data protection.

This situation, in the protection of privacy in the EU, in which privacy is subordinated to market, is accentuated further by the ECJ in the *PNR case*. The ECJ case-law in the PNR case has been criticized for *opening an important gap in the protection of personal data*. The findings of the court that the objective of the contested acts did not relate to the functioning of the internal market and thus fell outside the scope of the directive on data protection is hardly shocking. It is surprising that in the judgment there is a total silence of any reference to fundamental rights protected under the international law and binding for the MS (such as the ECHR) or under the Member States own constitutions. The practical result of such a silence of the Court is that the latest PNR Agreement adopted by the Council in October 2006 is even less protective of personal data than the one annulled by the ECJ. Therefore in a possible review of the directive it would be necessary to subordinate the market to the data protection and not the other way round.

### 5.2 Principles

The Directive is based on the *principles* of Council of Europe Convention (recital 11 of the preamble). Further the directive in Article 6 (1) lays down the core principles which require that the personal data must be:

- processed fairly and lawfully (Article 6(1)(a)),
- collected for specified, explicit and legitimate purposes (Article 6(1)(b)),
- adequate, relevant and not excessive in relation to the purposes for which they are collected (Article 6(1)(c)),
- accurate and where necessary kept up to date (Article 6(1)(d)),
- kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected (Article 6(1)(e)).

---

262 HATZOPOULOS, supra note 118, p.56.
263 HATZOPOULOS, supra note 118, p.56.
Furthermore the Directive in Article 7 provides for the *conditions under which the data processing can be legitimate*:

- if the data subject has unambiguously given his consent (7(a)),
- if it is necessary for the performance of a contract to which the data subject is party (7(b)),
- if it is necessary for compliance with a legal obligation (7(c))
- is necessary in order to protect the vital interest of the data subject (7(d)),
- if processing is necessary for the public interest (7(d)),
- if necessary for the legitimate interest of the public controller (7(f)).

These principles or conditions, under which the processing of the personal data can be legitimate, generally are sound, but some of them notably the principle of “consent” have its limits. The limits of this principle will be discussed in the next sections of this thesis.

The Directive further provides for, in Article 8, stricter rules for the processing of special categories of data (or the so called sensitive data) such as racial or ethnic origin, political opinion, or data concerning health or sex life (Article 8(1)).

### 5.3 Controller's obligations versus data subject rights

Under the Directive the most important are the **data subject**\(^{264}\) and the **controller**\(^{265}\). The Directive provides for several obligations on the data controller as well as accords some rights to the data Subjects. **Article 10 and 11 lays down the obligation for the data controller to provide the data subject with the following information:**

- identity of the controller (Articles 10(a) and of his representative, if any,11(a)),
- purpose of the processing (Articles 10(b) and 11(b),
- further information such as the recipients of the data, right to access and to rectify the data (Articles 10(c) and 11(c).

These obligations of the data controller are provided for in order to enable the data subject to perform their rights. **The data subject has the right:**

\(^{264}\) Article 2 (a) define the “data subject” an identifiable or identified subject.

\(^{265}\) Article 2 (d) defines “controller” as the “(…) natural person or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and the means of the processing of the personal data (…)”
• of access to data (Article 12),
• to object the processing of data relating to him (Article 14).
• not to be subject to a decision, which is based on automated processing of data, intended to evaluate certain personal aspects relating to him (Article 15).

Furthermore, the directive provides for the obligations of the data controller to maintain the confidentiality of the processing (Article 16) and data processing security (Article 17) and the obligation to notify the supervisory authority before carrying out any automatic processing operation intended to serve a single purpose (Article 18).

5.4 Transfer of data to non-EU countries

The transfer of personal data to destinations outside the Community may present dangers to the freedoms and rights to privacy, particularly where the standard of the data protection in the receiving country is poor or non-existent\textsuperscript{266}. Another problem may be the risk of circumvention of the local data protection law by the Community based-data protection controllers who may be tempted to store and process their holdings of personal data outside the community to take advantage of the lack of data protection law. Therefore, in order to address the challenge of cross border data flows and to prevent the circumvention of the data protection law the Directive applies a multi-option mechanism. The Directive permits the extra-territorial processing of data under several routes addressing the country as a whole (Article 25) and then offering a set of derogations (Article 26)\textsuperscript{267}.

5.4.1 Country Adequacy

When the controller is situated outside the EU and the personal data are transferred to countries outside the Community which are undergoing processing or are intended for processing after transfer the Directive (Article 25(1)) requires that “... the Third country in question ensures an adequate level of protection”. The criteria for determining the adequacy of the level of protection are not very clearly defined. The notion of adequacy is a variable concept depending on the circumstances surrounding the transfer of such data. Article 25(2) gives an indication of the circumstances to be taken into account in the assessment of the adequacy of protection required in the third country being:

\textsuperscript{266} BAINBRIDGE, supra note 29, 70.
\textsuperscript{267} BIRNHACK, supra note 5, p.9.
• nature of the data,
• purpose and duration of the proposed processing,
• country of origin and country of final destination,
• the rule of law both general and sectoral,
• professional rules and the security measures in that country.

Articles 25 (3) and Article 31 lays down the procedure of communication between the Commission and the Member States when a third country does not insure an adequate level of protection of personal data. If a third country does not ensure an adequate level of protection, the commission may require the Member States in question to take measures to prevent any transfer of data of the same type to the third country (Article 25(4)).

The reasoning behind the rules laid down in Articles 25 and 26 of the Directive is that without them the high standard the data protection would quickly be undermined given the ease with which the data can be moved around through the international computer networks. Thus, the goal is sound: adequacy of the third countries is important so to protect the interests of the European data subjects.

However, these provisions have raised many concerns and have been challenged many times in practice either due to the technological developments or the difficulty in adopting decisions that proclaims a third country not adequate for data protection. If we take into consideration the growth of telecommunications, in particular networks such as the internet, it is hard to see just how effective these provisions can work in practice. Whilst it is relatively easy to police the use of personal data by public authorities and large business organizations established within the community, it will be much harder to control misuse of personal data by others. These issues will be analyzed more in detail in Chapter 6.

---

268 BAINBRIDGE, supra note 29, p. 73.
Legal Problems with the Directive 95/46/EC

The Data Protection Directive has many legal problems. Some of its current rules are too complex and too strict at a general level (resulting in excessively stringent regulation beyond what is necessary to counter misuse), while others are too vague and open-ended (causing legal uncertainties and differences in application). This chapter analyzes some of the legal issues that arise under the Directive against the wider technical and legal backgrounds.

6.1 Difficulty in applying legal definitions [Article 2]

The clarity of the definitions in legal texts is crucial because ambiguities create uncertainties, loopholes and invite costly and time-consuming legal disputes. In the text of the Directive most problematic are the definition of the controller, the distinction between the “controller” and “processor”, (Article 2(d)-(e)) as well as the need to add some important notions to the Directive.

6.1.1 The definition of the controller [Article 2(d)]

There is a problem, in the definition in the Directive concerning the reference to “controllers” acting “alone or jointly with others”. This phrase (which was added to the definition by the European Parliament, late in the drafting of the Directive) lacks the clarity as to what this reference means. In particular, it could suggest that for some processing operations there can be more than one “joint controllers” (i.e. shared control). Moreover, this expression appears also in the newly adopted Framework Decision in the third pillar (Article 2(i)). However, this provision raises a lost of problems with regard to the application of many of the provisions in the Directive, which generally assume that there is one controller for any specific operation, and which requires this controller (singular) to ensure compliance with various requirements, such as the informing of data subjects, notification, allowing subject access, etc. The issue has also implications for the determination of the “applicable

---

269 KORFF, supra note 98, p. 245.
270 KORFF, supra note 98, p.29.
law” (Article 4) with regard to processing by (or within) groups of companies, when different companies belonging to the same group are established in different Member States.

6.1.2 “Data Controller” versus “Data Processor”

The Directive divides the universe of actors who process personal data into “data controllers and “data processors”. This classification of actors in “controllers” and “processors” has important consequences in a number of areas: first, most data protection obligations under the Directive must be met by the “controller”, second, in most cases “data controllers” (rather than data processors) are liable for data protection violations (Article 23) and third, “data processor” have a severely reduced role, because are supposed only to process personal data as directed by the controller. However, there is uncertainty about when a processor becomes a controller or vice versa, particularly in online environment and in business environment with highly complex structures.

In the context of Internet and electronic communications, the distinction between the “data controller” and “data processor” has proven to be a challenge. Identifying a data controller in an open network is difficult and the question raised is whether multiple controllers exist. The answer is that, in such a network, there may be multiple controllers.

For instance, e-mail traffic, may involve multiple controllers. Under the Recital 47 of the Directive, when an individual uses an e-mail service on the Internet, he should be considered as a controller of the personal data in the e-mail, since he determines the purpose and means of the processing. The Internet Access Provider (IAP) is also controller since it processes certain data such as the web site visited or the address of the POP/SMTP server to which the user connects, the time and duration of the connections ensured through its intermediary. The transmitter will be deemed the controller in respect of the processing of additional personal data necessary for the operation of the service. Finally, once the data is received or intercepted, the receiver or interceptor will become the controller.

Furthermore, as the SWIFT case shows, the highly complex structure of the businesses, particularly the financial sector, makes it difficult to determine in practice which part is the

---

271 KUNER, supra note 14, p. 70.
272 RAND Europe (2009), supra note 2, p. 36.
274 KUNER, supra note 14, p. 72.
“controller” and which is the “processor”. Accordingly the question raised is whether an entity is sufficiently involved in the determination of the purposes and means of the processing to be considered a controller.

When the Directive was enacted there was a much clearer distinction between the parties who control the processing of the personal data and other parties who only process personal data in behalf of others. However, the advances in computer technology and the scope of internet have largely caused this distinction to break down.

Accordingly, since the lack of clarity between the roles of “controller” and “processors” has substantial implication for legal compliance, these terms need to be clarified in the context of a possible review of the Directive.

6.1.3 The need to add some definitions to the Directive.

Several Member States (Austrian, German and Spanish laws etc.) during transposition of the Directive in their national laws define “anonymising” or “pseudonymising” (encoding) of personal data. The Problem is that the definitions given by various Member States show that the concepts are by no means clear-cut and indeed blends into each other. Therefore consideration should be given to add these definitions - in particular “anonymsing”\ “pseudonymsing” - to the list of definitions in the Directive. Also many other Member states define the concept of “blocking”. Moreover the terms “blocking” (Article 2 (c)) and “to make anonymous” (Article 2(k)) are defined in the new horizontal framework decision adopted under the third pillar in a similar way with the national definitions given in the national law which implement the Directive on data protection. Therefore the new revised Directive should include these definitions in list of definitions.

There is also the need to determine the expression of “transfer of data” to third countries (this will be discussed further in the next section of Article 25 and 26). It must be recognized that, the publication on web sites of certain information and their availability throughout the world create definitively a major privacy risk which justifies the application of the articles 25 and 26. So, we might imagine that certain duties of care would be imposed to the website

---

275 TREACY, supra note 121.
276 KUNER, supra note 14, p.71.
277 Ibid.
278 KORFF, supra note 98, p. 35.
creators and to their hosting providers and that the possibility of intervention by the public authorities ought to exist in case of major risks, for example if it is proved that people from a third country are systematically analyzing the profiles of individuals apart from their presence on the web in order to take actions against them or to publish their profiles.

6.2 Problematic aspects of the “Applicable Law” [Article 4]

The provisions of the Article 4 of the Data Protection Directive constitute the first set of rules in an international data protection instrument to deal specifically with the determination of the applicable law. The drafters of the previous International Instruments on data protection were unable to reach an agreement on applicable rules. Two factors inherently complicate the application of this article. The first complicated factor relates to the nature of the data protection law in relation to private international law. Data protection law straddles the boundaries between the public and the private law, criminal and civil law. It is very difficult to firmly place the data protection law within any one of the legal categories traditionally employed by the doctrine of the private international law. The second complicating factor is the nature of the information systems that the data protection law seeks to regulate. Many of these systems are increasingly difficult to link to one fixed geographical location, which the doctrine of the private international law tends to rely on an ability to make such links. Article 4 of the Directive 95/46/EC, first of all, tries to ensure that there are no (positive or negative) conflicts between the laws of the Member States, i.e. that to any one processing operation falling within the scope of the Directive one law of a Member State applies, and not more than one law (or no law) (Article 4(1)(a) and (b)) and second, tries to harmonize the Member States’ approach to transfers of personal data from their territories (i.e. from the territory of the Community) to other (“third”) countries (Article 4(1)(c)). Both aspects present legal problems that will be analyzed in the following sections.

6.2.1 Problems with applicable law between the EU Member States [Article 4(1)(a)]

The aims of the Article 4 (1)(a), as set down in the preamble of the Directive are twofold: to avoid the negative conflict between the laws of Member States, i.e. a situation in which the data subject finds himself outside any system of protection (no law is applied), and to avoid the positive conflict between the laws of the Member States, i.e., a situation in which the same data-processing operation is governed by the laws of more than one country\textsuperscript{282}.

However, as the Article 4 is worded it is unlikely that the second aim (i.e. to avoid the positive conflict) be met in some circumstances\textsuperscript{283}. The Directive is based on the assumption that there will be one controller for one data-processing operation. As we analyzed above (definition of “controller”) there could be occasions where exists two or more controllers (multiple controllers), each established in different Member States, for one specific operation. In such cases, taking into account the connecting factor (i.e. the controller’s place of establishment) for the determination of the applicable law, application of Article 4 would mean that one specific data processing operation is subject to different national laws.

A second, problematic aspect of Article 4 is that it is not clear concerning the extent of the territorial application of the Member State’s national data protection law\textsuperscript{284}. Article 4 ensures that a particular law applies in a particular situation, which can cause problems of jurisdictional collusion. Therefore in terms of legal certainty this Article should be clarified.

A third, problematic aspect with Article 4 is that the Member State in which a data controller is established will not necessary be the Member state in which the data subject affected by the processing is domiciled or resident. Thus, given the trans-border data flows in the era of the internet, data subject are likely to be increasingly forced to seek remedies under foreign law of another Member State for the protection of their data protection rights. The problem is that the data subjects are the weak part in the processing of personal data, and therefore they may face difficulties that they would not otherwise experience in seeking remedies pursuant to the national laws.

No doubt that the intention of the drafters of the Directive was to harmonize the respective data protection laws of the Member States and thus to reduce the above mentioned

\textsuperscript{282} BYGRAVE(2000), supra note, 279, p.7.
\textsuperscript{283} BYGRAVE(2000), supra note 279, p.7.
\textsuperscript{284} BYGRAVE(2000), supra note 279, p.8.
difficulties. However, studies on the implementation of the Directive found that there are serious problems in the application of these rules, which results in positive and negative conflicts of law between the Member States, which Article 4 of the Directive seek to avoid.\textsuperscript{285} The study point out that, the different application of the Directive by the EU Member States, is caused in part, by the excessive complexity of Article 4(1)(a), which is worded in such a complex terms that, it almost invites different (divergent) applications.

### 6.2.2 Problems with applicable law between the EU and Non-EU countries [Article 4(1)(c)]

A first problematic aspect of Article 4(1)(c), is that it gives rise to the possibility of “regulatory overarching” in an online environment. Bygrave describes the expression “regulatory overarching” as a situation in which “rules are expressed so generally and non-discriminatory that they apply \textit{prima facie} to a large range of activities without having much of a realistic chance of being enforced”\textsuperscript{286}. For instance, if an operator of the websites, established, say in India, set “cookies” onto the browser programs of those visiting their sites who are persons situated in EU, then the operator action meets the criteria of Article 4(1)(c), i.e. the operator would be processing personal data making use of equipment situated on the territory of EU Member States. This would mean that the processing would be governed by the data protection law of the EU Members State concerned.

Thus, in the online environment, the strict application of Article 4(1)(c) is likely to create a situation in which a large number of data controllers in third countries are supposed to comply with two sets of data protection rules that may not be harmonized: the rules of the EU/EEA Member State and the rules of the respective countries in which the controllers are established (e.g. India). Since under the Article 4(1)(c) the connecting factor for the application of the EU Member state law is the “equipment situated in a EU Member State” and since the notion of the “equipment” is a loose one, such that the equipments used in one data processing operation can be dispersed over several countries, then controllers might have to comply with a considerable multiplicity of national laws.\textsuperscript{287} Moreover, many controllers, (situated in countries lacking data protection rules) will be unaware of these

\\[\textsuperscript{285} \text{KORFF, } \textit{supra note} \text{ 98, p.46.}\]
\\[\textsuperscript{286} \text{BYGRAVE (2000), } \textit{supra note} \text{ 279, p.8.}\]
\\[\textsuperscript{287} \text{Ibid. p.9.}\]
compliance duties. Who is to draw the attention of data controllers in third countries to the provisions of Article 4(1)(c)? Accordingly, the DPAs are reluctant to extend the application of their national laws to situations in which they cannot effectively enforce them. As the Irish Data Protection Commissioner puts it, “we should not pretend to control what we cannot in fact control”.

Another problem is that, in online environment, it will be very difficult for a data subject or DPA to determine the location of the controller, let alone, to work out where the latter is established. Moreover, given that the legal parameters of the concept of the establishment are far from clear, at least in the context of the online networks, there will be difficulties in working out, if an establishment exists.

The above mentioned problems questions many of the assumptions on which the directive is based. The enforcement of the rights for the data subjects is based in the assumption that location of data controller is determined. The enforcement of the rights laid down in the directive for the data subject (i.e. the principle of consent (Article 7(a), the right for information (Articles 10 and 11), right to access to data (Article 12), right to object (Article 14)) are based in the assumption that location of data controller is determined. If data subjects do not know that data on them are being processed by whom, they cannot effectively exercise their rights and thus, data protection becomes illusory.

6.2.3 Problems with the wording of Article 4(2)

The critics to the point 2 of Article 4 of the Directive 95/46/EC can be best summarized by the remarks of the UK Information Commissioner (data authority) which says:

“… Directive requires that a data controller outside the EU appoints a representative in the Member State where processing takes place. What is the purpose of this? There is no apparent basis on which the Commissioner could take action against a representative for a breach of UK law by a data controller established outside the EU.”

Ibid.
288
289
290
KORFF, supra note 98, p.57.
291
KORFF, supra note 98, p.57.
292
Ibid.
293
Ibid.
294
KORFF, supra note 98, p.57.
In sum, the “applicable law” rules in the Directive need to be re-drafted in such a way as to remove ambiguities in the present text, if one of the main purposes of the Directive is not to be defeated.\footnote{KORFF, supra note 98, p.47.}

6.3 Reconciling Data Protection with Freedom of Expression [Article 9]

The relationship between the data protection and the freedom of expression provided for in European Human Rights Instruments (ECHR and EU Charter of the Fundamental Rights)\footnote{ECHR provides for the Protection of Privacy and Family Life in Article 8 and the freedom of expression in Article 10, while the Charter of Fundamental Rights provides for the protection of personal data in Article 8 and freedom of expression in Article 11.} is a complex and problematic one. Directive lays down some exceptions which aim to reconcile the “right to privacy with the rules governing freedom of expression” (Article 9). The exceptions and derogations laid down in the Directive should go no further than “necessary” to achieve this aim, i.e. that the fundamental right to data protection as provided for by these European Instruments and ensured by Directive should only be limited to the extent “necessary” to protect the competing Charter-protected interest, freedom of expression.

However, Article 9 of the Directive is somewhat at odd with these instruments. The Directive unjustifiably stipulates that this relates only to “processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression”: the right to freedom of expression is guaranteed by Art. 10 ECHR and Art. 11 of the Charter to “everyone”, not just to journalists, artists and writers.\footnote{KORFF, supra note 98, p.121.}

In the Satamedia Oy case\footnote{Judgment of the Court of 16 December 2008, in case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, not yet reported.}, the ECJ was asked to rule on the interpretation of Article 9 of the Directive, i.e. on the interplay between the fundamental rights of data protection and privacy and the fundamental right to the freedom of expression. The question raised in the preliminary ruling, was whether activities such as, the collection of data from documents in the public domain held by the tax authorities and processed for publication for commercial purposes, can be regarded as the processing of personal data carried out ‘solely for journalistic purposes’ within the meaning of Article 9 of the Directive. The ECJ held that, it is necessary to interpret notions of journalism broadly and that Article 9 of the Directive...
apply not only to media undertakings but also to every person engaged in journalism. Therefore, the ECJ concluded that, such activities must be considered as activities involving the processing of personal data carried out ‘solely for journalistic purposes’ under the Article 9 of the Directive, i.e. exempted from general principles of the Directive.

Even thought the ECJ interpret the journalism broadly, it does not interpret the journalism as an important notion of freedom of expression as broadly as to include everyone as required by ECHR and the Charter of Fundamental Rights, but limits it only to the category of persons “engaged in journalism”.

Therefore since Article 9 of the Directive has raised wide differences and serious problems in the way the press, and matters relating to freedom of expression generally are dealt with in the Member States in the national laws transposing the Directive, this matter needs to be further examined in detail, with reference to both data protection- and freedom of expression standards, as developed at EC and wider European level and to the case-law of the European Court of Justice and the European Court of Human Rights in particular. However, it is clear that, in any case, Article 9 of the Directive will need to be rephrased.

6.4 Data Subject rights to object [Article 14(a)]

Under the Directive the most important figures are the data subject and the data controller. The Directive provides for several obligations on the data controller (Articles 10 and 11) as well as accords some rights to the data Subjects (Article 12 and 14). Under Article 14(a) the data subject has the right:

“… to object at any time on compelling legitimate grounds … to the processing of data relating to him… Where there is a justified objection, the processing …may no longer involve those data”.

There are number difficulties with the meaning and the purpose of the Article 14 (a). A part from wondering what “compelling legitimate grounds” are, this also begs the question of

---

300 KORFF, supra note 98, p.119.
301 BYGRAVE (2000), supra note 279.
301 Emphasis added.
“justified by whom”? The controller, the data subject or the supervisory authority?\(^{302}\) The provision could have a number of meanings. Much depends on the meaning of “legitimate” – does it mean “lawful” or “justifiable.”\(^{303}\) It would be reasonable to suppose that objecting on “legitimate grounds” must mean when the processing envisaged is contrary to the provision of the directive and not simply because the data subject does not want his data processed. But if this so, then the best and most effective approach would be to alert the Supervisory Authority which could perform its supervisory duties. The recitals do not help in understanding the meaning or the purpose of the Articles 14(a) because recital 45 is expressed in very similar wording\(^{304}\).

6.5  Problems with data-flow to third countries [Articles 25 and 26]

As we analyzed above, the Article 1(2) of the Directive lays down the principle of free movement of the data within the Community. This free movement is the direct effect of having an effective data protection law within the Community. However, transfer of personal data to destinations outside the Community may present dangers to the freedoms and rights to privacy, particularly where the standard of the data protection in the receiving country is poor or non-existent\(^{305}\). Another problem may be the risk of circumvention of the local data protection law by the Community based-data protection controllers who may be tempted to store and process their holdings of personal data outside the community to take advantage of the lack of data protection law. Therefore, in order to address the challenge of cross border data flows the Directive and to prevent the circumvention of the data protection law applies a multi-option mechanism.

The Directive addresses the challenge of cross-border data flows in Articles 25 and 26. Article 25 prevents, as a principle, all data flow to third countries “without an adequate level of protection”. If this is not the case, Article 26 gives certain alternative paths for transfer. The reasoning behind these rules is sound: without them the standards of the data protection within the EU would quickly be undermined given the ease with which the data can be moved around through the international computer networks.

---

\(^{302}\) BAINBRIDGE, supra note 29, p. 66.
\(^{303}\) BAINBRIDGE, supra note 29, p. 67.
\(^{304}\) BAINBRIDGE, supra note 29.
\(^{305}\) BAINBRIDGE, supra note 29, p.70.
However, these rules are outmoded and no longer appropriate in an era of globalization\textsuperscript{306}. If we take into consideration the growth of telecommunications, in particular networks such as the internet, it is hard to see just how effective these provisions can work in practice. Whilst, these rules seek to protect the European citizens, the sheer quantities of personal information transferred oversees may undermine this\textsuperscript{307}. Therefore, these rules have been criticized as outmoded and cumbersome.

In the following will be discussed three issues: first, the lack of the definition of the concept of “transfer” of personal data, second, the problematic aspects of “country adequacy”, and third, the limits of the concept of “consent”, as a criteria for legitimizing the transfer of data to third countries and the limits of the “appropriate contractual clauses”.

6.5.1 The Directive does not define the concept of “transfer” of personal data

The directive does not define the concept of “transfer” of personal data, even though, this concept is important both for the transfer of data within the EU, but, most importantly, in determining whether restrictions under EU law on transferring personal data to third countries are applicable\textsuperscript{308}.

In the past, it was less of a problem to determine whether the restrictions on data transfers were applicable, since the data transfer was often accomplished by physical means that were easily ascertainable. However, in the internet age, personal data are constantly being made accessible to recipients outside the EU via the internet, and it is often not clear, if, for instance, placing of data on the internet, which can be accessed by someone browsing World Wide Web should be considered to be a data transfer under Directive 95/46/EC. Moreover, given the importance of this concept, several Member States (e.g. Germany) define such concept\textsuperscript{309}.

The ECJ case-law is of little help in clarifying this concept and has raised more confusion than clarification of this concept concerning the scope of “transfer to third countries”. In the Lindqvist case\textsuperscript{310}, among the prejudicial question raised by the Swedish Court to the ECJ was whether the articles 25 and 26 of the Data Protection Directive applicable to web sources. The European Court’s answer was in negative: ECJ found that placing material on a

\textsuperscript{306} RAND Europe (2009), supra note 2, p. 33.
\textsuperscript{307} RAND Europe (2009), supra note 2, p. 33.
\textsuperscript{308} KUNER, supra note 14, p.80.
\textsuperscript{309} Ibid.
\textsuperscript{310} Case C-101/01, Criminal Proceedings against Bodil Lindqvist, [2003] ECR I-12971, paras 88-90.
server located in the EU, which was accessible worldwide via the internet, did not constitute international transfer under Article 25 of the Directive.

The arguments used by the Court might easily receive objections\textsuperscript{311}. Under the judges’ opinion the transfer of data means “active transmission” and not “consultation apart from abroad”. This distinction between “transmission” and “consultation”, from a technological point of view is quite ambiguous.

What is the difference between, on one side, the situation where a sender, through his/her computer programming, send data to a recipient or, on the other side, the one where by another programming, the sender makes accessible certain data to this recipient? The difference between the “push” and the “pull” systems makes no sense, except if the sender has no technical possibility to avoid the transfer by blocking the access\textsuperscript{312}. In the case of a web site, accessible through the Internet, the creator of the web site has willingly made the data fully available because has the possibility to restrict the access. The second argument is still weaker. Following the judges in Linqvist, if a data transfer exists, it occurs from the hosting service and not by the web site creator\textsuperscript{313}. This argument might not be accepted. The hosting server is not a data controller but a data processor insofar he is acting on behalf of the web site creator. Anyway, this argument does not contradict the existence of a transfer to third countries\textsuperscript{314}.

The Lindqvist Judgment not only directly contradicts the opinion of a number of DPAs who had held prior to the decision that the creation of web sites constitutes “transfer”\textsuperscript{315}, but also creates the risk that companies may regard Linqvist, as a carte blanche to ignore the EU legal restrictions on data transfers.

It must be recognized that, the publication on web sites of certain information and their availability throughout the world, creates definitively a major privacy risk, which justifies application of the articles 25 and 26 of Directive. Accordingly, certain duties of care should be imposed to the website creators and to their hosting providers. In addition, the possibility of intervention by the public authorities ought to exist in case of major risks, (for instance) when placing on the internet a large amount of data and for business purposes\textsuperscript{316}.

\textsuperscript{311} POULLET, supra note 41, p.9,
\textsuperscript{312} Ibid, p.12.
\textsuperscript{313} Case C-101/01, Bodil Lindquist, [2003] ECR I-12971, para.61.
\textsuperscript{314} POULLET, supra note 41, p.9.
\textsuperscript{315} KUNER, supra note 14, p.82.
\textsuperscript{316} KUNER, supra note 14, p.83.
6.5.2 Problematic aspects with country “adequacy”

Under Article 25(1) the transfer of data to third countries is forbidden except if an “adequate protection” is offered by the third country. The goal of this provision is sound: adequacy of the third countries is important so to protect the interests of the European data subjects. However, the notion of adequacy is a variable concept depending on the circumstances surrounding the transfer of such data. A third country may have a higher level of protection exceeding the requirement of the Directive, in a given sector (e.g. healthcare and financial service providers in US), but not in others.

Another issue raised is how effective these provisions are. The Directive offers a modest threat, in case a third country is not found to ensure an adequate level of protection. Under Article 25(4), the Member states “shall take the measures necessary to prevent any transfer of data of the same type to the third country in question”. This language leaves some interpretative leeway to the Member states. What are the necessary measures, to prohibit the transfer of such data? One can argue that, these measures should be proportional to the inadequacy level of the third country: i.e. if a third country does not offer an adequate level of protection, for instance, of medical data then the limitation on transfer should be narrowed down to such data. Nevertheless, the Directive realizes that the inadequacy finding can raise difficulties and so, it allows negotiations with the third country, (Article 25(5)). Importantly, the data collectors operating in inadequate third country can rely on other avenues of data export, namely, many derogation laid down in the Article 26.

Moreover, the system for assessing the adequacy of third countries is too limited. Thus far, the avenue of country adequacy is used only in few cases. After 15 years, only 5 non-EU countries have been found to have adequate legal framework: Switzerland, Canada, Argentina, Guernsey, Isle of Man and Jersey (See Annex I). Current and emerging trade powers such as China, India, Brazil, Japan and Russia are not included and US is only covered through “Safe Harbor” Agreement (and to a lesser extent the Agreement on the transfer of PNR data to the Bureau of Customs and Border Protection).

317 BIRNHACK, supra note 5, p. 10.
318 E.g. Health Insurance and Portability and Accountability Act (HIPAA), RAND Europe, (2009), supra note 2, p. 34.
319 BAINBRIDGE, supra note 29, p.72.
320 BIRNHACK, supra note 5, p.10.
321 Ibid.
322 RAND Europe (2009), supra note 2, p. 33.
In addition, the adequacy rules are considered to be inappropriately focused. There are cases in which the harmonization with the Directive of the third countries laws, would automatically lead to worse level of protection for the European data protection subjects.\(^{323}\)

In conclusion, the “country adequacy” is lacking effectiveness, either due to technological developments (the age of internet) or due to the difficulties that EU can find (both on political and trade accounts) not to declare a country adequate for data protection, as it is illustrated by the PNR case and the subsequent developments. The result of these difficulties is that the objectives to offer high level of protection to EU citizens pursued by the Articles 25 and 26 of the directive are undermined.

### 6.5.3 Limits of “Consent” as a criterion for legitimizing the data processing/transfer [Article 26(1)]

Article 26(1) lists several options which permit the export of personal data to a third country, that does not have adequate protection. The first situation is when the data subject has given his “unambiguous consent” for the transfer to third states (Article 26(1)(a)).

“Consent” is a crucial element for a data protection regime. It is based on the notion of “human dignity” and “privacy” as a control, namely, only the data subject can decide if, when and to what extent to open his or her virtual private sphere to other entities.\(^{324}\) But the “consent”, as a criterion to legitimize the processing of personal data, has its limits, because it is a highly volatile concept and subject to manipulation.\(^{325}\)

The question raised is: what is the cumulative meaning and effect of the consent? If controllers of data can easily gain the data subjects consent, doesn’t this mean it is an empty term? The concern is that the consent is a hollow promise of control to data subjects. If the concern materializes, then the consent-based conception of privacy is dangerous: instead of a promise of control, it de facto means the opposite, surrender of control. The promise of control turns unto illusory, or worse, deceit. For these reasons, several privacy scholars abandoned the notion of consent as a central pillar of privacy law in general and data protection in particular.\(^{326}\)

It can be questioned whether the Directive requirement of consent as a ‘freely given specific and informed indication of his wish’, (Article 2(h)) is often realized.\(^{327}\) For instance, there

---

\(^{323}\) Ibid, p.34.

\(^{324}\) BIRNHACK, supra note 5, p. 10

\(^{325}\) Ibid, p.11.

\(^{326}\) BIRNHACK, supra note 5, p. 10

\(^{327}\) RAND Europe (2009), supra note 2, p. 30.
are risks associated with obtaining consent, in the context of electronic commerce, since there is increased danger that the subject might not have been fully informed or might not really understood what he is consenting to. Moreover, the measures taken by the Community regulations to protect the consumers against the effects of the unfair standard terms, in contracts concluded with professionals (i.e. business-to-consumer contracts), is a recognition that consumer consent with standard terms, is often very relative and that it should be possible to set unfair terms aside, even if the consumer originally consented to them.

In the international transfers of data, assuming that the consent has been “unambiguously” given (Article 26(1)(a)), the question raised, is what happens in the post-consent period?

The Directive attempts to deal with the shortcomings of the “consent” by defining the consent (Article 2) and by requiring that the processing is allowed subject to the data subject’s unambiguous consent, (Article 7(a)) and (Article 8(2)(a) and Article 26(1)(a).

However, these safeguards provided for to deal with the limits of the consent, address to some extent, the collection and the processing of the personal data within the EU, but not the case of transfer of data to third states. For extra-EU transfer of data the Directive requires the “unambiguous consent” of the data subject, but, this term is ambiguous and leaves a loophole: once the data is transferred it is almost impossible for the EU data subject to enforce his or her rights if violated. Thus, EU law sets a prerequisite for the export, but does not provide effective enforcement beyond the initial point of consent. The EU citizen lacks the real power to enforce his rights outside the EU, especially when the third country at stake does not have an adequate data protection regime.

The limits of the “consent” as legal basis for international transfer of data were best illustrated by the SWIFT case. The Brussels-based SWIFT transferred personal banking information to the US government without the knowledge (and the “consent”) of the EU individuals. The processing of the data by SWIFT was in breach of the Data Protection

---

328 KUNER, supra note 14, p.60.
331 BIRNHACK, supra note 5, p.11.
332 Ibid.
333 SWIFT, supra note 71.
334 TREACY, supra note 121.
Directive\textsuperscript{335}, nevertheless, revealed the limits of the consent as a criterion, legitimizing the processing, which can be easily circumvented or abused.

In the light of the above considerations, effective data protection is better served, by ensuring that, the data subject’s access to efficient tools to enforce his rights, than by overemphasizing the legitimizing capacity of consent on specific instances of data processing\textsuperscript{336}.

\textbf{6.5.4 Limits of the “appropriate contractual clauses” [Article 26(2)]}

Another way that the Directive (Article 26 (2)) permit the export of the personal data is in the form of “appropriate contractual clauses” or Binding Corporate Rules (BCR) offered to multinational corporations, which requires the European approval. BCR are a Code of Conduct adopted and implemented by a multinational corporation regarding the extra-European processing of data. The benefit of BCR is that a European employee working for a multinational firm operating under a BCR in a third country that lacks any data protection regime, will nevertheless enjoy some protection for his personal data. But BCR option suffers from several problems. First, the process of approval is rather long, cumbersome and expensive. Second, BCRs are limited in their scope to particular transfers of data which are in the hands of the given corporations and as a consequence they do not offer a universal solution to all data protection issues. Third, by definition, multinational firms are likely to push for a lower level of data protection. Forth, enforceability and compliance are difficult to achieve\textsuperscript{337}.

\textsuperscript{336} RAND Europe (2009), \textit{supra note} 2, p. 30.
\textsuperscript{337} BIRNACK, \textit{supra note} 5, p.13.
7 Initiatives for the review of the Data protection Directive 95/46/EC

This chapter examines the recent developments in the context of the review of the Directive. It looks first at the European Commission evaluations of the Directive and next at the (past and current) initiatives calling for the amendment of the Directive.

7.1 Evaluation of the Directive 95/46/EC by the EU Commission: Amendments premature

European Commission has evaluated the Directive 95/46/EC for the first time in 2003. In its report, the European Commission described that there is a clear lack of harmonization, but stated that there was no reason yet to come to an amendment of the directive and that it was necessary to make a better use of the existing legal framework. The European Commission in that report stated that in the course of the consultations conducted “few contributors explicitly advocated the modification of the Directive”.

While the Commission only mentions the proposal for the amendment of the Directive submitted jointly by Austria, Finland, Sweden and UK, interestingly enough, does not mentioned the fact that it commissioned a study on the implementation of the Data Protection Directive. The study, which was carried out from October 2001 to September 2002 by Professor Korff, University of Essex (UK), aimed at providing the basis for the review of the implementation of the directive which the Commission was required to undertake. The report consisted of three parts Part I divided into Part I.A (comparative study of the national laws) and Part I.B (implications for the internal market), Part II sound and image data) and Part III. Summary, Conclusions and Recommendations.

From the Draft Final Report the Commission accepted only the Part I.A (comparative study of the national laws) and not the other Parts, i.e. findings, conclusions and recommendations. The reason given by the Commission was that the report was submitted late (it should be

---

339 Ibid. p.7.
340 KORFF, supra note 98.
341 KORFF, supra note 98.
submitted in April/May 2002 in fact it was submitted in July 2002)\textsuperscript{342}. However, given that, the part accepted and published by the Commission was also submitted late, it follows that the main reason was not the delay (otherwise Commission should have rejected the Study \textit{en block} and not in selective way), but the fact that the non-accepted parts of the Draft Final Report were highly critical and recommended amendments of the Directive. However, the author published all the parts of its report hoping to “assist in the debate on the future of the Framework Data Protection Directive … on the future of data protection generally”\textsuperscript{343}. This thesis draws extensively on that publication and we are very much grateful to Professor Korff for the contribution given in the wider debate on these issues.

The 2003 Report published by the Commission contained a \textit{Work Programme for better implementation of the data protection Directive}. The Commission in 2007 analyzed the Directive in a Communication on the follow-up of the above mentioned Work Programme\textsuperscript{344}. The Commission considered that, Directive “fulfils its original objectives” and therefore does not envisage “submitting any legislative proposal to amend the directive”\textsuperscript{345}. However, this positive assessment of the Commission for the Data Protection Directive is not shared by others, and many voices (in the past and currently) call for its amendment.

7.2 \textit{Past initiatives for the review of the Directive 95/46/EC: Sweden “Misuse Model” of data protection}

The Data protection Directive is based on the “\textit{processing model}”, which applies to any processing of personal data and is focused in the \textit{pre-emptive ‘avoidance of risk’}. But it is widely felt (in particular in Northern Europe), that \textit{on the one hand}, data protection is (or has become) \textit{too technical and prescriptive}, while \textit{on the other hand} it is said that the rules are \textit{insufficiently attuned to the specific conditions and requirements of controllers}\textsuperscript{346}. This opinion is also shared by other countries, UK, Nederland, and Germany. The German

\textsuperscript{342} \textit{KORFF, supra note 98, p.1.}
\textsuperscript{343} \textit{KORFF, supra note 98, p. 2.}
\textsuperscript{345} \textit{Ibid.} p.9.
\textsuperscript{346} \textit{KORFF, supra note 98, p.239.}
Government report on the “modernization of data protection” also feels that data protection law (in particular in that country) has become too technical and legalistic.\footnote{KORFF, supra note 98, p. 239.}

**This has led to calls for a new approach.** The Swedish Government suggests that the rules should aim at “countering abuse”, rather than at (pre-emptive) “avoidance of risk”.\footnote{Ibid.} Therefore, Sweden proposed the so-called “misuse model” which applies to certain categories of data that can be misused.\footnote{WONG, “The Shape of Things to Come: Swedish Developments on the Protection of Privacy”, Script-Ed, Vol. 2, No. 2, pp. 107-124, 2005, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=924634&download=yes} The “misuse model” is defined as a regulatory approach that seeks to enhance the efficacy of the rules by simplifying and focusing them on preventing misuse of personal data.\footnote{BYGRAVE, “The 1995 EC Directive on Data Protection under Official Review- Feedback so far”, (2002) Privacy Law and & Policy Reporter, Volume 9, pp.126-129.} This model separates the data processing into two categories: one including applications not structured to facilitate retrieval of personal data (such as word processing and email) and the other including databases and other data structures created for easy retrieval of data. Processing of information in the first category would only be punished if it resulted in harm to the data subject, while the processing of the information in the second category would be subject to the current protections of the Directive.\footnote{Kingdom of Sweden: Constitutional Privacy Framework, EPIC and Privacy International, Survey on Privacy and Human Rights 2005, pp. 663-664, available at the: http://www.privacyinternational.org/survey/phr2005/PHR2005swed-ven.pdf}

Sweden, since 1998 has been pushing for a pan-European adoption of “misused model” and has advanced several amendments of the Directive. But, since there are various models and approaches to the data protection within EU Member States it is not easy to find support for one model by the majority of the Member States. However, in 2002 Sweden, supported by Austria, Finland, and the United Kingdom, managed to propose amendments to the Directive, even though less radical than its original misuse model.\footnote{Data Protection Directive (95/46/EC), Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom, Explanatory Note, September 2002, available at the website: http://www.dca.gov.uk/ccpd/dpdamend.htm (last visited 3.04.2009)} These amendments were done in the framework of the 2003 Commission Report on the implementation of the Directive. According to the explanatory note of the proposal, the proposal “intended to help the Commission in its consideration of the changes that are needed to the Directive in the light of Member States' experience with operating it”.\footnote{Ibid.} The proposal contained amendments to provisions on special categories of data (Article 8), provisions on the
information for data subjects (Article 10 and 11), data subject rights of access (Article 12), Notification provisions (Articles 18 and 19) and transfer of data to third countries (Article 25 and 26). But, the proposal did not lead to an amendment of the Directive and the Commission in its 2003 Report, argued that “these proposals for amendments concerned only a small number of provisions … leaving most of the provisions and all of the principles of the Directive untouched”.

The model proposed has its limits and shortfalls, but, the argument of the Commission for not accepting them is not convincing. We do not think that the amendment of 8 out of 34 Articles of the Directive can be considered amendments of a small number of provisions. Moreover, these amendments did not leave the principles of directive unchanged because they aimed at changing the current “data processing model” in which the Directive is based, into a “misuse approach” or a mix of both.

Nevertheless, Sweden has not abandoned its model and it is probable that in the future will present new proposals. Moreover, in Sweden in first January 2007 entered into force the amendments to the Personal Data Act (PDA) adopted in 1998 to implement the Directive 95/46/EC which introduced into the PDA the “misused model”. These amendments were considered by the 29WP as “an adoption to reality”. Moreover, the Study of the RAND Europe (May 2009) recommended the adoption of a Charter for Effective Interpretation of some Articles of the Directive under the above mentioned model, adopted in Sweden.

Even though the “misuse approach” has many limits, yet, we think that in the context of a future review of the Directive this approach can be adopted in part, to simplify some unnecessary too complex and too detailed articles of the Data Protection Directive.

7.3 The current voices calling for the review of the Directive 95/46/EC

As we analyzed in the the previous chapters the original objectives of the Directive focused broadly on protecting the right to privacy in the processing of personal data, while ensuring

---

354 Data Protection Directive (95/46/EC), Proposals for Amendment, supra note 352.
356 See for a critique to the “misuse model” Wong, supra note, 329, p.111.
359 RAND Europe (2009), supra note 2, p.41.
the free movement of such data within the European Union. Fuelled in part by technological and commercial developments since its adoption in 1995, voices in some quarters are increasingly questioning the ability of the Directive to fit for its purpose and are calling for the Directive to be reviewed. These Voices includes Institutional Voices (EDPS, UK’s Information Commissioner Office (ICO) and various think-thinks (RAND Europe), scholars and experts.

Even European Commission, either or not pushed by these voices, has also employed several activities in this respect. First, in June 2008 the Directorate General, Justice Freedom and Security has commissioned a comparative assessment study to “…identify the challenges for the protection of personal data…and give guidance on whether the legal framework of the Directive provides appropriate protection or whether amendments should be considered in the light of best solutions identified”.

Second, Commission has installed a Data Protection Expert Group (DPEG), to make a comparative study on privacy challenges in the light of the new technology and to make proposal for the future review of the Directive 95/46/EC for data protection. The group's mandate is to assist the Commission in the preparation of legislation in the data protection area, and to help it in the definition of its policy. The DPEG will help the work of the Commission to identify the challenges posed on the data protection in the EU by the development of the new technologies, globalization and public security issues, taking into account the new Institutional Framework laid down by the Lisbon Treaty and to put forward proposals for the response to these new challenges. The DPEG held its first meeting on 4 December 2008. The DPEG has identified 5 issues for further examination: first, the implementation of the general framework of the Data Protection (Notification, application, mutual recognition), second the data collection in a globalized world (i.e. applicable law, the international transfers of the data), third the legal issues (i.e. definitions and scope), forth, the access of the governments to the data and the limits of such access and fifth, the

---

363 THOMAS and WALPORT, supra note 360, p. 59.
information of the consumers and the protection of the individuals rights\textsuperscript{365}. It was decided that the next meeting of the DPEG would be on 19 February 2009 but, the European Commission decided to dismantle the DPEG and to broaden the consultation on the review of the 1995 data protection Directive\textsuperscript{366}. The DPEG was dismantled because Mr. Alex Turk, the French Data Protection Authority President and the Chairman of Article 29 Working Party, has complained about the biased structure of the Group Explaining, to a French Senate Committee, that the group was composed of “four-fifths of personalities representing American interests”\textsuperscript{367} The next Expert Group on data Protection is expected to be reformed as a larger and more representative group. However, what will change is only the composition of this expert group but the mission and the mandate of the next DPEG will not change.

Third, on 19 and 20 June 2009, the European Commission organized a Personal Data Conference "Personal data - more use, more protection?" to look at new challenges for privacy\textsuperscript{368}. The objective of the conference is to “give the opportunity to various stakeholders to express their views and questions on the new challenges for data protection and the need for an effective information management strategy in the EU”\textsuperscript{369}. The conference is part of the Commission’s open consultation on how the fundamental right to protection of personal data can be further developed and effectively respected, in particular in the area of freedom, justice and security\textsuperscript{370}. This initiative of the Commission does not constitute an official EC review of the Data Protection Directive. As we analyzed the official position of the Commission, for the time being is that the Directive need not be amended.\textsuperscript{371} However, from the Commission practice follows that, before presenting proposals for

\textsuperscript{365}Compte rendu de la première réunion du groupe d’experts change de réfléchir au cadre légal de la protection des données dans l’union Européenne- dit «GEX PD » 4 Décembre 2008, disponible dans le siteweb: http://www.senat.fr/leg/ppr08-203.html


\textsuperscript{367}Mr. Alex Turk explained to the French senate Committee on 3 February 2009, that 4 out of 5 Members of the DPEG are representatives of the American Companies or American Law Firms, and therefore he asked to nominate European experts. See for further information : Le Sénat de la République Française, Proposition de Résolution Européenne sur la nomination, par la Commission Européenne d’un Group D’Experts sur la protection des Données, Sénat, Session Ordinaire de 2008-2009, Séance du 6 février 2009, website: http://www.senat.fr/leg/ppr08-203.html


\textsuperscript{369}\textit{Ibid}

\textsuperscript{370}\textit{Ibid}

amendments of a directive the Commission has, as a first step, commissioned Experts Groups to inform the debate and to advise the Commission in the preparation of its proposal. This is the case for the Commission proposal for the amendments to the e-Directive. In this case (but not only) the Commission has based its arguments in favour of the proposal (Explanatory Memorandum of the amendments to the e-Directive) on the results and on the recommendation of the studies carried out by the Expert Groups. Therefore, we assume that the establishment of the new Expert Group on data protection with a clear mission and temporary mandate can be interpreted as a first step in the direction of the review of the data protection directive. These initiatives of the Commission are to be welcomed and sustained hoping that they will be followed by other steps in the direction of a possible review of the Directive 95/46/EC. Now we turn to analyze the initiatives of EDPS and the ICO.

7.3.1 European Data Protection Supervisor

In his opinion of 25 July 2007 on the future of the Directive 96/46/EC, the EDPS invited the Commission to start the thinking about a future framework on data protection, which will not, by definition, be fundamentally different from the present one. EDPS distinguished among others the following relevant perspectives of such a process:

- Interaction with the technology,
- the global privacy and jurisdiction issues dealing with the trans-border data flows with the effects outside the territory of the EU,
- data protection and,
- Lisbon Treaty.

These perspectives must be seen in the light of fundamental changes of the European Union—increase in the free flow of information between the MS and between the MS and third countries— and of an evolving information society with more and more characteristics of the surveillance society.

---


374 Ibid. point 6.
EDPS states that, the changes of the Directive will be in the longer term, but “a clear date for a review to prepare proposals leading to such changes should already be set now”. Such a date would give a clear incentive to start the thinking about future changes already now”\(^\text{375}\).

Several activities have been employed since by other actors, either or not inspired by this suggestion of the EDPS. European Privacy and Data Protection Commissioners’ Conference, held in Edinburgh, on 24 April 2009 has discussed this issue\(^\text{376}\) and the UK Information Commissioner’s Office has commissioned a study from the RAND Europe to support these discussions.

### 7.3.2 The UK Information Commissioner’s Office (ICO)

The UK Information Commissioner, Richard Thomas has voiced concerns in many occasions that, the European data protection act is out of date, bureaucratic and excessively prescriptive\(^\text{377}\). He told an International Conference in Cambridge, that:

“[T]he European data protection legislation needed updating to meet new challenges posed by online information… It is showing its age and failing to meet new challenges to privacy such as the transfer of personal details across international borders and the huge growth in personal information online. It is high time the law is reviewed and updated for the modern world”\(^\text{378}\).

In order to provide food for thoughts and to stimulate debate, ICO commissioned RAND Europe to conduct a review of the Directive 95/46/EC. The Report of RAND Europe was published in May 2009\(^\text{379}\). It found that, as we move towards an increasingly global,


\(^{379}\)RAND Europe (2009), supra note 2.
networked environment, the Directive, as it stands, will not suffice in the long run\textsuperscript{380}. Accordingly, the Report recommended that the “Directive should be explicitly included in the list of laws to be reviewed as part of the Better Regulation Agenda”\textsuperscript{381} and offered an Alternative Regulatory Model to remedy the shortcomings\textsuperscript{382}.

The themes of the Report were discussed at European Commissioner’s Spring Conference held in Edinburgh, in April 2009. Richard Thomas in his speech at that Conference said that: “We are equally clear that any reform will take many years, but the debate must start somewhere. That debate has started here in Edinburgh today”\textsuperscript{383}.

Based on the conclusions of the RAND Europe Report, he stated, that the Directive has general and special weaknesses which applies both to the text of the Directive and its implementation. He summarized some of the general weaknesses of the Directive as follows:\textsuperscript{384}

- The approach is now outdated – in terms of both technology and modern regulatory approaches. Technology has moved on massively in the last 20 years and the Directive is a “Mainframe Directive”,

- The regulation has also moved on. “Good” laws are those which are clear about their objectives are focused and proportionate in the problems they address, provide incentives and deterrents for maximum “self-enforcement” by organizations to achieve standards at or above the minimum level, have effective enforcement mechanisms; and avoid financial and operational burdens which cannot be justified.

- the Directive has insufficiently clear objectives and insufficient focus on detriment, on risk and on enforcement in practice,

- It is also widely seen as excessively bureaucratic and burdensome, and too prescriptive. Detailed rules tell organizations “How” to do things, with less attention to “What” they should be achieving or their own responsibility for achieving it\textsuperscript{385}.

Therefore, he concluded that the Directive has sharp critics and “there are real risks that others will articulate weaknesses with a shriller tone than mine and press for change which will not be welcome”\textsuperscript{386}.

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{380} Ibid. p. 41.
\item\textsuperscript{381} Ibid. p. x.
\item\textsuperscript{382} Ibid. pp.40-60.
\item\textsuperscript{383} ICO (2009), supra note 376.
\item\textsuperscript{384} ICO (2009), supra note 376, p. 2.
\item\textsuperscript{385} ICO (2009), supra note 376.
\end{itemize}
\end{footnotesize}
8 Tentative solutions to the legal challenge: Prospects for the construction of a global data protection regime

This thesis highlights the long-standing and wide-spread concern to protect privacy and related interests, particularly in the face of development of the I.C.T. As was analyzed in the previous chapters, the regulatory response to this concern in the form of data protection laws have emerged in many countries. The overall picture of data protection laws and initiatives around the world, over the past years indicates a slow, but gradual and steady expansion. At the time of writing 74 countries have already enacted data protection laws of some sort or are part of regional initiatives (OECD, Council of Europe, EU and APEC) or have made steps to join them (See Annex 1).

While the most far-reaching of these laws are still European, readiness to establish at least rudimentary regulatory equivalents is increasingly global.

Nevertheless, this thesis also highlighted numerous points of difference between the various data protection regimes. Different jurisdictions regulate data protection in different ways, have different preferences as to the mode of regulation and provide different remedies. The divide between the US and Europe is a stark example.

Since privacy is understood differently in the EU, US, APEC and elsewhere, the main challenge for the privacy is to construct a global data protection regime, which can be achieved either by choosing the best understanding of privacy, or by harmonizing the current privacy concepts. **This is a political and legal challenge.** The competition to choose the best understanding of privacy is a tough one mainly between the EU and the US as the two titans of privacy frameworks, but APEC is also emerging as data protection superpower and need to be taken into account in the future privacy developments.

Therefore, it is pertinent that the final chapter of the thesis, attempt first, to analyze more in detail the legal challenge of the privacy and data protection, namely, the possibilities for achieving greater harmonization of data protection regimes across the globe and second, to propose some alternative solutions to tackle this legal challenge.

---

386 ICO (2009), *supra note* 376.
Many factors and variables promote or slow down the construction of a global data protection regime. The analysis shows that it is extremely doubtful that we will see, at least in the short term, major progress with respect to harmonization at the global level. This is due not simply to the strength of ingrained ideological/cultural differences around the World, but also to the lack of a sufficiently strong dynamic and representative International body to bridge these differences (such the World Trade Organization-W.T.O.)\(^{387}\). The W.T.O. is occasionally touted as such a body. Yet, its ability to negotiate a broadly acceptable agreement on the data privacy issues will be hampered by its commercial bias. Its ability to negotiate quickly and effectively is also in doubt given its apparent tardiness during Doha Round of negotiations in crystallizing policy with respect to electronic commerce.

Since the slowing down factors for the construction of universal data protection regime may prevail at least in the short and medium term, from the EU data protection point of view, remains two other solutions: \textbf{first, the regional harmonization}, that is, to bring the data privacy regimes of non-EU countries in line with its preferred model\(^{388}\). \textbf{The second solution is the extraterritoriality} that is, extending the Extraterritoriality of the EU data protection rules, even though it would remain politically controversial and would raise the problem of enforceability of the decisions\(^{389}\). These solutions are tentative solutions because their realization depends on the dynamic nature of the field and of each of its components (law, commerce, technology, global politics) and the possible interference of unexpected factors (e.g., in the way that 9/11 September affected the field).

\section*{8.1 Promoting factors for a regulatory consensus on data protection at the global level}

The very nature of the issue at stake, i.e., information and personal data, requires a global solution. Information easily crosses the borders. Digital networks, namely the Internet enables a constants flow of data. Under the circumstances of the resource (information) and the technology at stake, a local solution, through the national law is bound to be defeated. A country may exercise its sovereign legitimate power to create a system of data protection, but this system can be circumvented by the creation of foreign extra-territorial data havens. Since the problem cannot be addressed at the national level, many factors push in the

\(^{387}\) BYGRAVE (2004), \textit{supra note} 9, p.347.

\(^{388}\) BYGRAVE (2004), \textit{supra note} 9, p. 348.

\(^{389}\) REID, \textit{supra note} 60, p. 489.
direction of establishing a global data protection regime. In the following will be analyzed some of these promoting factors.

8.1.1 The creation of international instrument: a growing need for a global approach

The international/regional instruments, considered either as hard law (Council of Europe Convention No. 108 and EU Directive) or soft law (OECD Guidelines, UN Guidelines, APEC Privacy framework), have a common features, in that they promote the dissemination of the data protection laws, establish a common set of principles and raise awareness. These initiatives, irrespective of their weaknesses are the foundations of a global data protection regime. They indicate a slow but nevertheless steady process of globalization of the data protection standards, composed of the dissemination data protection laws and their substantive convergence. The general principles laid down in those instruments reflect an embryonic development of a global consensus, taking account of the increasing flow across frontiers of personal data undergoing automatic processing. These instruments show the common interest to reconcile fundamental but ‘competing values’ such as privacy and free flow of information. They had a double effect, somehow paradoxical: on the one hand their broad principles have generated a new flow of national legislation and in this respect they have been used as a sort of international minimum standard level for data protection. On the other hand, their wide acceptance could be regarded as a sign that national approaches were not sufficient anymore and that global regulations should be worked out.

Convention No. 108 has binding force and requires embodying the principles of data protection in national law, but does not oblige the contracting parties to establish institutional mechanisms allowing independent investigation of complaints. The OECD Guidelines are only soft law and provide for no procedural means to ensure that the Guidelines actually result in effective protection of individuals. The UN Guidelines did not increase in a significant importance at the global level for the protection of the privacy. EU Data

---

390 REID, supra note 60, p.8.
391 Ibid.
392 DUMORTTIER and GOERMANS, supra note 18.
393 Ibid, p.12.
Protection is an engine for the globalization of the protections law but, as it currently stands have a lot of weaknesses.

This leads to the conclusion that, although international instruments have shown their importance in the world-wide protection of personal data, they are not sufficient as such to safeguard a comprehensive and appropriate personal data protection in the context of the digital economy\textsuperscript{394}.

However, these initiatives have contributed to establish at least a rudimentary regulatory equivalent at global level and therefore they can be considered a promoting factor for regulatory consensus on data protection in the global level.

### 8.1.2 International flow of data from the EU and the US: Safe Harbour privacy principles.

As is analyzed in the previous chapters there are different approaches on data protection between the EU and US which gave rise to disputes between the two Jurisdictions over the transfer of data (\textit{PNR}\textsuperscript{395} and \textit{SWIFT cases}\textsuperscript{396}). While the US government is subject to data privacy laws\textsuperscript{397}, it is the lack of a concerted regulation in the private sector that the Commission will not recognize the US as a “safe” country\textsuperscript{398}.

A compromise was reached in 2000 through the “Safe Harbour” Agreement\textsuperscript{399}, which entered into force on 30 November 2000. The safe harbour recognized seven privacy principles concerning notice, choice, onward transfer, security, data integrity, access and enforcement. These principles allow the US companies that complies with them to lawfully receive personal data from the EU.

Even though, this solution can be criticized for its self-regulatory nature and the lack of the actual effectiveness, \textbf{it has the merit that it managed to inject into the USA privacy legal system some data protection principles enshrined in the EU Data protection Directive}, which contributed to narrow the existing gap between the two titans of data protection.

\textsuperscript{394} DUMORTTIER and GOERMANS, \textit{supra note} 18, p.13.
\textsuperscript{395} \textit{PNR case, supra note} 21.
\textsuperscript{396} Society for Worldwide Interbank Financial Telecommunication.
\textsuperscript{397} Privacy Act 1974.
\textsuperscript{398} REID, \textit{supra note} 60, p.495.
jurisdictions. Therefore, the Safe Harbour Principles can be considered a promoting factor for the construction of a global data protection regime.

8.1.3 Directive 95/46/EC: A soft mechanism of legal globalization

Directive is the most successful and comprehensive international legal instrument of data protection laws. It is currently the leading force of globalizing data protection. There is sufficient evidence to determine that the directive has become not only a source of comparative law or a source of inspiration, but an effective mechanism to raise the level of data protection worldwide and that it is doing so better than other mechanisms.\(^{400}\)

First, the Directive binds 27 EU Member States and 3 EEA countries, Iceland, Lichtenstein, and Norway. Second, the Western Balkan countries (Albania, Bosnia and Herzegovina, Croatia, FYROM, Montenegro and Serbia) based on Stabilization and Association Agreements with the EU have to approximate their laws to the EU Acquis, including the approximation of the national legislation on data protection to the Directive 95/46/EC.

Third, the directive has a wider global impact. There is ample evidence that the directive has influenced the policy makers around the world. Data protection laws of many countries (Australia, Hong Kong, Israel, Japan, and South Africa) are modeled under the Directive. In some cases, the Directive provided merely another legislative model (Australia, Hong Kong, Israel, Japan, and South Africa), in other cases it tilted the contemplated data protection regime in a third country towards the European standard (New Zealand, China), and yet in other cases the impact was stronger, in that it was the main reason for enhancing data protection legislation in a third country (such as Dubai).\(^{401}\)

This evidence indicates that the EU has managed to raise concrete interest in various countries to adopt data protection laws (or amend data protection laws) so to adhere to the EU standards. The process is slow and faces local resistance and political attempts to search for other less burdensome alternatives that also provide less protection for data subjects. The


\(^{401}\) Dubai adoption of an EU-like data protection regime seems to be a case where the Directive was the sole reason of enacting the law. Moreover Dubai is the first Arab country to enact a data protection law in 2007. See, BIRNHACK, M. D., “Soft Legal Globalization: The Role of the EU Data Protection Directive in the Emerging Global Data Protection Regime. Tel Aviv University law School, Law Faculty Papers, Draft-Paper, February 2008, p.26.
APEC Framework is an example of such a regional attempt, though it is unlikely to prevail\(^{402}\).

The Directive has a crucial role to play. The adequacy mechanisms spread the European view more efficiently than the non-binding Council of Europe Convention no.108, UN Guidelines or the OECD Guidelines and no doubt that it is more effective than the APEC scheme, which currently lacks any serious treatment of the data flows outside the APEC economies.

As the evidence shows countries seek the EU’s stamp of approval for their own interest, so to enable easier data transfers between their local countries and the EU and to gain symbolic political capital.

However, beyond the motives that push the countries to adopt data protection laws under the EU model, the role played by the Directive, as soft mechanism of legal globalization\(^{403}\), can be considered a promoting factor for the constructions of a global data protection regime.

### 8.1.4 2005 Montreux Declaration of Data Protection Commissioners: working towards adopting a Universal Convention on Data Protection

The Montreux declaration of 2005 adopted by the International Conference of Data Protection and Privacy Commissioners, from countries which have data protection laws, appeal to the UN to prepare a legally binding instrument which clearly sets out in details the rights to data protection and privacy as enforceable human rights.

Other Conferences held in London, Montreal and Strasbourg 2008 recall the Montreux declaration and urges to adopt a Universal Convention on data protection. Therefore, the Montreux declaration and its initiatives is a strong promoting factor for constructing a global data protection legal regime.

\(^{402}\) BIRNHACK, supra note 400, p.27.

\(^{403}\) BIRNHACK, supra note 400.
8.2 Slowing down factors for regulatory consensus on data protection at the global level

Many factors slow down the process of achieving the consensus on data protection at the global level. The main factor is the fact that the US does not share the European philosophy of the data protection, a gap that is not easy to bridge.

8.2.1 Lack of any clear and generally agreed definition of privacy

As we analyzed in the previous chapters there is lack of a clear and generally agreed definition of what privacy means. Privacy is a contested legal concept, with several understandings and more misunderstandings, covering distant areas of human activities. Privacy is actually shorthand for a complex bundle of issues, ranging from dignity to discrimination, and rooted in our need to control what we tell others about ourselves.

The difficulty in articulating what privacy is and why is important to protect, causes a lot of legal problems. First of all, the law fails to identify the central interests at stake which the privacy law is asked to redress. Therefore, since legal protection of privacy depends upon a conception of privacy that informs what matters are protected and the nature and scope of the particular protections employed, the lack of a clear concept of what exactly privacy is creates difficulties when making policy, and as a result the legislation fail to pass both at the national level and most importantly at the global level.

Therefore, the confusion in the definition of the privacy is a slowing down factor for constructing a global data protection legal regime.

8.2.2 Differences between the data protection regimes: the divide between the EU and the US

The main slowing down factor for the construction of a global data protection is the difference between data protection regimes around the World, especially the stark divide between EU and the USA data protection regimes.

The US law has not recognized a general right of data subjects regarding their personal information and choose not to recognize a general category of informational privacy. The Atlantic divide reflects two distinct views as to informational privacy. While the European

---

404 BIRN Hack, supra note 5, p. 1.
405 BIRN Hack, supra note 5, p. 2.
view treats data protection as a human right, reflecting the control of a person over his or her identity or dignity, the American view, treats data as crucial for the efficient functioning of the market and a tradable good, with only limited sector-based protection accorded to the data subjects.

While the US government is subject to data privacy laws\textsuperscript{406}, it is the lack of a concerted regulation in the private sector that the Commission will not recognize the US as a “safe” country\textsuperscript{407}. Therefore the Directive in its extra territorial ambit was bound to conflict with the American approach as it did in fact in many cases, concerning the disputes between the two Jurisdictions over the transfer of data (\textit{PNR\textsuperscript{408}} and \textit{SWIFT cases\textsuperscript{409}}).

Therefore, the divide between the EU and the US is considered as the main slowing down factor for constructing a global data protection legal regime.

\textbf{8.2.3 The lack of a strong representative International body to adopt rules}

The difficulty for achieving progress with respect to harmonization at the global level is due not simply to ideological/cultural differences around the World, but also to the lack of a sufficiently strong, dynamic and representative International body to bridge these differences\textsuperscript{410}. The World Trade Organization (W.T.O.) is occasionally touted as such a body.

For instance, EU Proposed to go for global solutions within the framework of the WTO, and the WTO has accepted to include data protection in its work programme on trade related aspects of electronic commerce\textsuperscript{411}. The objective is the agreement on basic principles allowing for free flow of personal data in World Wide electronic commerce, whilst respecting the individuals right to privacy and thus ensure trust and confidence in electronic commerce.

However, WTO ability to negotiate a broadly acceptable agreement on the data privacy issues will be hampered by its commercial bias. Its ability to negotiate quickly and effectively is also in doubt given its apparent tardiness during Doha Round of negotiations in crystallizing policy with respect to electronic commerce.

\textsuperscript{406} Privacy Act 1974.
\textsuperscript{407} REID, supra note 60, p.495.
\textsuperscript{408} \textit{PNR case}, supra note 21.
\textsuperscript{409} Society for Worldwide Interbank Financial Telecommunication.
\textsuperscript{410} BYGRAVE (2004), supra note 9, p.347.
\textsuperscript{411} DUMORTTIER, and GOERMANS, supra note 18, p.13.
Therefore, it follows that the lack of a sufficiently strong, dynamic and representative International body to adopt rules can be considered as a slowing down factor for the construction of a global data protection regime.

### 8.3 Conclusion: It is difficult to achieve a regulatory consensus at global level on data protection

The analysis of the promoting and slowing down factors for the construction of a global data protection regime, shows that it is extremely doubtful that we will see, at least in the short term, major progress with respect to harmonization at the global level.

This is due to the fact that slowing down factors analyzed above are actually prevailing and they will do so in the near future.

The lack of a clear definition of privacy and the stark divide between EU and the USA and now APEC privacy regimes, are structural slowing down factors which will take time to bridge and therefore, it is difficult to expect to overcome them in the near future.

Since it is likely that the negative scenario be realized, from the EU data protection point of view, remains two other solutions: **first, the regional harmonization**, and the **second solution is extending the extraterritoriality of the Directive 95/46/EC**. These two alternatives will be analyzed in the next sections.

### 8.4 Two tentative solution from the EU data protection perspective: Harmonization on regional level and extraterritoriality

As we discussed above, it is difficult to achieve a regulatory consensus at global level on data protection. However, from the EU perspective it is possible to envisage two possible solutions: harmonization on the regional level and the extraterritoriality. These solutions are tentative solutions because their realization depends on the dynamic nature of the field and of each of its components (law, commerce, technology, global politics) not to mention the possible interference of unexpected factors (e.g., in the way that the 9/11 September affected the field).
8.4.1 Harmonization on regional level

From the EU data protection perspective, the regional harmonization, means, to bring the data privacy regimes of non-EU countries and regions in line with its preferred model\textsuperscript{412}. This is not something new because the current Directive 95/46/EC has already played a central role as a soft legal globalization, but the challenge for the EU is to go further in process and attempting to bring rival concepts of information privacy of other countries (USA) and regions (APEC) to converge with the European model and thus attempting to set global rules of information privacy modeled under the European model.

**However, a large question mark, hangs over the EU ability to achieve this objective.** This is partly, because of the recent emergence of APEC as a potential competitor in the role of “data privacy superpower” and partly because of the weaknesses of the Directive, notably Article 25 and 26 of the Data Protection Directive.

Spreading the EU’s principles on data protection thus faces a tough competition. In addition to the past competition with the USA, there is an emerging competition between the EU’s model and other regional models such as the APEC.

How these principles and rules are implemented constitutes a test for the Directive international credibility and success. The regime of transborder data flows to third countries (Articles 25 and 26) seems to be caught between “a rock and a hard place”\textsuperscript{413}: if properly implemented, the regime is likely to collapse from the weight of its cumbersome, bureaucratic procedures. Alternatively, it could well collapse because of large scale avoidance of its proper implementation due precisely to fears of such procedures.

8.4.2 Claiming extraterritoriality of the EU data protection law

The second solution is extending the extraterritorial application of the EU data protection rules, that is, abolishing the principles of nationality and territoriality, even though it would remain politically controversial, especially with the USA and would raise the problem of enforceability of the decisions\textsuperscript{414}.

\textsuperscript{412} BYGRAVE (2004), supra note 9, p.348.
\textsuperscript{413} BYGRAVE (2004), supra note 9, p. 348.
\textsuperscript{414} REID, supra note 60, p.489.
Reid articulated this solution, in the context of the online data protection privacy in 2004, but, that solution can be extended to cover other sectors of data protection as well. He argues that what is required is a framework that offers identical protection in as many jurisdictions as possible, with an effective body to police and enforce rules. He argues that, EU is such a body and by taking a harder line on protecting individual rights, a Union “founded on the principle of ... respect for human rights and individual freedoms” it could offer the solution. This means that the EU act unilaterally to ensure an adequate degree of protection for its citizens.

However, Data Protection Directive avoids the issue of extraterritoriality, by prohibiting transfers of data outside the EU, unless the third country “ensures an adequate level of protection.” Actually there are five countries that are declared safe (see Annex I). But, if the extraterritoriality of the EU law is extended, then this prohibition of the Directive would be redundant, therefore would be amended to allow for the free transfer of data from the Community. Article 4 of the Directive also would need to be amended in order to abolish the territorial principle (i.e. the territorial connecting factors such as the establishment of the controller within the EU and the equipment for processing data situated in the EU), which limits the territorial application of the Directive 95/46/EC, only within the EU territory.

Our reflections concerning the possibility of extending the extraterritorial application of the Directive 95/48/EC, naturally lead to the following question: whether claiming extraterritoriality of this Directive is a viable solution under the EU privacy Law and International Law?

To answer this question it is useful to explore a two-steps analysis: first, we should analyze cases of extraterritorial application of the EU privacy rules and second the compatibility of the extraterritorial application of the EU data protection rules with the International law (i.e. WTO).

8.4.2.1 Extraterritoriality in the EU Data Protection Laws

The first step in our analysis is to analyze whether the extraterritorial application of the Directive 95/46/EC is a viable solution under the EU data protection law. To this end, it is analyzed the case of the extraterritoriality of the Directive 2002/58/EC as well as three legal
constructions or doctrines established by the ECJ case-law concerning the extraterritorial effect of the EU competition law: “single economic entity” doctrine, “implementation doctrine” and the “effects” doctrine,

8.4.2.1.1 Extraterritoriality of the Directive 2002/58/EC

Even within the EU legal framework of data protection, one can find cases of legal acts which have extraterritorial application. This is the case of the extraterritoriality of the Directive 2002/58/EC. The provisions of the Directive 2002/58/EC target all the electronic communication services without taking into account the nationality or the establishment of their providers. In that sense, one might speak clearly about the extraterritoriality of this Directive.

Some of the services covered by the Directive might be offered to a subscriber or a user inside the EU from a provider located outside the EU, for example as internet access provider. In that case the text states clearly that the European Directive is applicable.

Article 5.3 of the Directive 2002/58/EC which severely limits the use of the electronic communications services, for providing access to information stored into the terminal equipment is applicable to all electronic communication service providers, no matter where these service providers are established. Moreover, no territorial limits are restricting the scope of the provisions of this Directive.

Thus, the criterion fixed by the Directive 2002/58/EC is not the same as the criterion of establishment retained by the Directive 95/48/EC and will thus permit an extraterritorial effect of the Directive 2002/58/EC.

However, as we mentioned above the Directive 95/46/EC avoids the issue of extraterritoriality, by limiting the territorial scope of its application, (Article 4) and by prohibiting transfers of data outside the EU, unless the third country “ensures an adequate level of protection” (Article 25.1).

Now, that the analysis shows that Directive 2002/58/EC has extraterritorial effect, but the Directive 95/46/EC fix other criteria, which avoids the extraterritoriality, the next stage in

---

418 POULLET, supra note 41, p. 12.
419 Ibid.
our analysis is to examine to what extent the ECJ case-law, concerning the extraterritoriality of the Community Law can be helpful in this respect.

In fact, the Commission decisional practice and the ECJ corpus of case-law, for many years extended the extraterritorial application status\(^{420}\) of the EU law in the field of competition law, through the use of three “legal constructs” or doctrines. First, the “single economic entity doctrine”, which has as its underpinnings the nationality principle\(^{421}\), second, the “implementation doctrine”, which is based on the territorial principle\(^{422}\) and third the “effects doctrine”, which extends the subject-matter jurisdiction\(^{423}\) to all situations where the economic effects in the EU of anti-competitive actions, taken abroad are immediate, reasonably foreseeable and substantial\(^{424}\).

The two former doctrines are well-established doctrines of the EC Law. Indeed it is now established that the Articles 81 and 82 of the EC Treaty (after the entry into force of the Lisbon Treaty Articles 101 and 102) apply no matter where an undertaking has its headquarters or where the agreement has been concluded\(^{425}\).

However, it remains unresolved whether the “effects doctrine” enjoys the same status\(^{426}\), since there is an absence of formal recognition by the ECJ of the “effect doctrine”. This doctrine is recognized by the European Commission in many decisions. Nevertheless, the fact that the “effects doctrine” has not been formally recognized by the ECJ will have no bearing on the ability to assert subject-matter jurisdiction over the non-EU undertakings located outside the EU. The economic entity and the implementation doctrines are more than adequate in this respect\(^{427}\).

In the following sections are briefly analyzed these three doctrines as well as the extent to which they can be used to extend the extraterritorial application of the Directive 95/46/EC.

---


\(^{421}\) Territorial principle allows a nation to subject to its jurisdiction conduct which has a sufficiently close link to its territory.

\(^{422}\) On the basis of the nationality principle the Commission has jurisdiction over the ratione personae over the activities of undertakings having their seat in the EU.

\(^{423}\) There are subject-matter jurisdiction and the enforcement jurisdiction. Subject matter-jurisdiction is the right which States or institutions possess to make their law applicable to the activities, relations or status of persons and to the interests of persons in property. Such jurisdiction is exercised by the enactment of legislation such the former Articles 81 and 82 of the EC Treaty ( now the articles 101 and 102 of the Lisbon Treaty) and Directive 2002/58/EC, or by the laying down the rules by administrative agencies or by the courts. Enforcement jurisdiction, on the other hand, is the power of a state or body such as the EC to induce or compel compliance or to punish non-compliance.


\(^{425}\) GERADIN, supra note, 420, p.4.

\(^{426}\) GERADIN, supra note 420, p.1.

\(^{427}\) GERADIN, supra note, 420, p.1.
8.4.2.1.2 “Single economic entity” doctrine in EU Law

The issue of extraterritoriality was originally dealt with by the European Court of Justice, in the field of competition which developed the “single economic entity” doctrine. *Dyestuffs case*\(^{428}\) represents the seminal ECJ case-law as far as the single economic entity doctrine is concerned. In the *Dyestuffs* the Commission had investigated a possible cartel and found that Imperial Chemical Industries Ltd. (ICI), a company registered in the UK (at that time was not EC Member state), by instructions given to subsidiaries established in various EEC Member States, engaged in a concerted practice and was fined.

On appeal before the ECJ the parent company challenged the jurisdiction of the Commission to impose fines on undertakings established outside the Community\(^ {429}\) and asked to impose fines to its subsidiaries established within the Community\(^ {430}\).

AG Mayras also urged to uphold the decision of the Commission under the ‘effects doctrine’. The ECJ upheld the Commission decision, but opted for the “single economic entity” doctrine. Thought the effects of the relevant practices were briefly alluded to, a response on the application of the “effects doctrine” was shied away from, preference being accorded to handing down a judgment based on the established doctrine of a single economic entity\(^ {431}\).

This doctrine allows that parent and subsidiary companies be treated as single company for the purpose of competition law, that is allowing companies established outside the Community to be punished, where they have subsidiaries within the Community\(^ {432}\). Therefore, on the basis of the nationality principle, jurisdiction was asserted over non-EC parent undertakings by attributing liability to them for the illegal price fixing of the dyestuffs by their subsidiaries located in the EC over which the non-EC parent undertakings exercised control. Similar, reasoning is also to be found in the ECJ’s *Continental Can judgment*\(^ {433}\).

**Applying such a doctrine to the Directive 95/46/EC would allow it to be enforced against any company that had offices, branches or subsidiaries within the EU.** Many US companies have such links and as such the Community could enforce its privacy

---

\(^{428}\) Case, C-48/69, Imperial Chemical Industries Ltd (ICI) v Commission (Dyestuffs) [1972] ECR 619.

\(^{429}\) Case, C-48/69, supra note 428, para. 125.

\(^{430}\) Case, C-48/69, supra note 428, para. 131.

\(^{431}\) Case, C-48/69, supra note 428, para.126.

\(^{432}\) Case, C-48/69, above point 428, at [134-141].

requirements against them\textsuperscript{434}. Therefore, the finding that there is a single economic entity doctrine may bring a non-EC undertaking within the scope of the EC data protection provisions.

However, this doctrine has the inherent limitations in that it could not be stretched to catch purely non-European players\textsuperscript{435}. In this respect, the remedies are the "implementation doctrine" and notably "effects doctrine".

8.4.2.1.3 The "Implementation doctrine" in the EU Law

The "implementation doctrine" represents an alternative legal construct as far as the extraterritorial application of EC competition law is concerned. Pursuant to this doctrine, which is based on the territoriality principle, agreements and practices fall within the purview of Articles 81 and 82 EC, irrespective of where they find their geographic origin, the decisive factor being whether they are implemented within the European Community and trade between Member States is affected.

In Wood Pulp case\textsuperscript{436} the Commission investigated alleged price fixing and fines were imposed upon many undertakings, all of whom had the registered office outside the Community, but had some form of establishment within the Community.

All the applicants contested the Community’s jurisdiction to apply its competition rules to them, given that all the applicants had their registered offices outside the Community. The applicants maintained that the Commission had misconstrued the territorial scope of the Article 81 of the EC Treaty and that the application of that Article to them:

"…would be contrary to public international law which precludes any claim by the Community to regulate conduct restricting competition adopted outside the territory of the Community merely by reason of the economic repercussions which, that conduct produces within the Community."\textsuperscript{437}

Again the court was encouraged by the AG Darmon\textsuperscript{438} to adopt the ‘effects’ doctrine to establish extraterritorial jurisdiction. But again the ECJ avoided discussing the ‘effects’

\textsuperscript{434} REID, supra note, 60, p.500.
\textsuperscript{435} GERADIN, D., REYSEN, M. AND HENRY, D, supra note 420, p. 5.
\textsuperscript{437} Joint Cases, C-89, 104, 114, 116, 117 and 125 to 129/85, supra note 436, para. 6.
\textsuperscript{438} Opinion of Mr Advocate General Darmon delivered on 7 July 1992, Joined cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 and C-125/85 to C-129/85, E.C.R. [1993] P. I-1307.
directly and considered ‘implementation doctrine’. According to the ECJ in its Wood pulp judgment⁴³⁹:

“16. It should be observed that an infringement of Article [81], such as the conclusion of an agreement which has had the effect of restricting competition within the common market, consists of conduct made up of two elements, the formation of the agreement, decision or concerted practice and the implementation thereof. If the applicability of prohibitions laid down under competition law were made to depend on the place where the agreement, decision or concerted practice was formed, the result would obviously be to give undertakings an easy means of evading those prohibitions. The decisive factor is therefore the place where it is implemented.

17. The producers in this case implemented their pricing agreement within the common market. It is immaterial in that respect whether or not they had recourse to subsidiaries, agents, sub-agents, or branches within the Community in order to make their contacts with purchasers within the Community.”

According to Wood pulp case, therefore, the criterion as to the implementation of an agreement is satisfied by mere sale within the Community, no matter the location of the sources of supply and the production plant and where the anti-competitive arrangement was entered into. A corollary of this is that Community jurisdiction is triggered by the simple fact that products are directly sold to Community purchasers.

In this case, ECJ adopted the “implementation doctrine” and did not recognize the “effects doctrine”. As a result, the ECJ found that the Community’s jurisdiction was covered by the territorial principle, as recognized by the International law⁴⁴⁰:

“18. Accordingly the Community’s jurisdiction to apply its competition rules to such conduct is covered by the territoriality principle as universally recognized in public international law”.

However, the “implementation doctrine” alone could not catch those that collect data online, but having no connection with the community. An ‘effect doctrine’ which is wider in scope would remedy this problem.

**8.4.2.1.4 The ‘effect doctrine’ in EU Law**

The “effects doctrine” for the purposes of asserting extraterritorial jurisdiction is based on the economic effects felt within the Community. The effects doctrine has been recognized and accepted by the Commission in various Decisions⁴⁴¹ and Guidelines⁴⁴².

---

⁴³⁹ Wood Pulp Case, supra note 436.
⁴⁴⁰ Wood Pulp case, supra note 436, para.18.
In *Wood Pulp Decision*\(^{443}\), for example, the Commission held that the relevant pulp producers and trade associations had infringed Article 81 (1) EC all of which had their registered offices outside the Community. The Commission explicitly made reference to the effect of the agreements and practices on prices announced and/or charged to customers and on resale of pulp within the EC in order to assert jurisdiction. The Commission Guidelines (2004) on the effects on trade concept contained in Articles 81 and 82 of the Treaty foresee that these articles apply:

“...irrespective of where the undertakings are located or where the agreement has been concluded, provided that the agreement or practice is either implemented inside the Community, or produce effects inside the Community.”

Moreover, the Commission recently made explicit reference to the *Wood pulp judgment* in order to assert jurisdiction over a global price-fixing cartel for lysine involving undertakings from third countries\(^{444}\).

Though the “effects doctrine” has been recognized and accepted by the Commission, the ECJ has never handed down a judgment explicitly affirming the doctrine, preferring to rely on the more politically uncontroversial “single economic entity” and “implementation doctrines.”

On appeal before the ECJ, the Advocate-General Mayras in *Dyestuff case*\(^{445}\) and AG Darmon in the *Wood pulp Case*\(^{446}\) urged the ECJ to uphold the decision of the Commission under the ‘effects doctrine’. They espoused the effects doctrine reflecting a belief among several Advocate-Generals that the doctrine should become an established concept of EC law. AG Darmon opined that “there is no rule of international law which is capable of being relied upon against the criterion of the direct, substantial and foreseeable effect”\(^{447}\).

Despite the Advocate-General’s fervent view that the effects doctrine should become a cornerstone of EC competition law when applying it extraterritorially, the ECJ subsequently relied on the implementation doctrine to assert jurisdiction over undertakings located outside the Community. The ECJ’s coy stance vis-à-vis the *effects doctrine*, however, could be

\(^{442}\) Commission Notice -Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, (2004), O.J.C. 101/81, para.100.


\(^{446}\) Opinion of Mr Advocate General Darmon delivered on 7 July 1992, Joined cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 and C-125/85 to C-129/85, E.C.R. 1993 Page I-01307.

\(^{447}\) Opinion of Mr Advocate General Darmon, supra note 446, para.57.
attributed to the fact that Europe’s political elite at that time vociferously criticized the doctrine when employed by the US antitrust authorities.\(^{448}\)

Nevertheless, in the field of merger control, the European Court of First Instance would seem to have endorsed the effects doctrine. In *Gencor case\(^{449}\) the territorial scope of the ECMR (Merger Regulation) vis-à-vis a proposed concentration notified by undertakings whose registered offices and mining operations were outside the Community was at issue. The applicants challenged the Commission’s assertion of jurisdiction before the CFI. The CFI held, using language evocative of that of Advocate-General Darmon, that:

“[the] [a]pplication of the [Merger] Regulation is justified under public international law when it is foreseeable that a proposed concentration will have an immediate and substantial effect in the Community.”\(^{450}\)

The fact, however, that the ECJ has thus far fudged on handing down an unequivocal ruling on the effects doctrine as such means that the effects doctrine as a concept of Community law remains unresolved\(^{451}\).

However, the approach taken by the ECJ in *Wood Pulp case* could have some implications for the protection of data privacy. By collecting the data outside the Community an easy way to circumvent the new protections would be opened. However, if the collection of data was seen as the implementation of a decision to breach privacy laws, and collection was deemed to take place when it was transferred, as opposed to being received, could the Community claim the jurisdiction under the *Wood Pulp* Jurisprudence?

The answer is in affirmative. In *Wood Pulp case*, the Court emphasized the “global dimensions” of the wood pulp market and second that Article 81 EC was aimed at practices that may effect trade or restrict competition within the Community\(^{452}\). Similar concerns arise in relation to the privacy notably in internet which is “global” and that the inability to enforce data privacy laws may have a negative effect upon common market.

Thus, in the vast majority of cases, notably the privacy in internet, the fact that the “effects doctrine” has not been formally recognized by the ECJ will have no bearing on the ability to assert jurisdiction extraterritorially in the data protection. The economic entity and

---

\(^{448}\) GERADIN, D., REYSEN, M. AND HENRY, supra note 420, p.5.


\(^{450}\) Case T-102/96, *Gencor*, supra note 440, para. 90.

\(^{451}\) GERADIN, D., REYSEN, M. AND HENRY, supra note 420, p.7.

\(^{452}\) Wood Pulp Case, supra note 420, para.12.
implementation doctrines should be more than sufficient. In this regard, whether one applies the implementation doctrine or the effects doctrine similar outcomes should normally be reached, although it is arguable that the latter doctrine is wider in scope.

Therefore, the community may claim jurisdiction over those which breached any data protection rules on the same ground as used in *Wood Pulp*, whether it is called an “effect doctrine” or not.

Another argument against the extension of the Competition law jurisprudence to the data protection law was that competition law is based upon the Treaty Articles (Article 81 and 82 of the EC Treaty) and the data protection was not. Fortunately, with the entry into force of the Lisbon Treaty this difficulty is already overcome, because the Lisbon Treaty provides for in Article 16 of the TFEU, the right to the data protection.

Thus, despite the fact that the Directive 95/46/EC avoids the extraterritoriality, in the light of the “single economic entity” doctrine, “implementation doctrine” and “effect” doctrine, its extraterritorial effect can be extended outside the EU territory and thus it is viable solution under the EU Law.

8.4.2.2 Compatibility of privacy laws which have extraterritorial effects with the WTO Rules

As we mentioned above, besides the Directive 2002/58/EC, laws which have extraterritorial application can be found in other national privacy rules:

- 1998 US COPPA (Children Online Privacy Protection Act),
- 2003 US SPAM Act which also has extraterritorial effect.
- Another case in the American law (even though not in the privacy law, but relevant to our analysis of extraterritorial effect of national law) is the case of the Intellectual Property (IP) by the USA which used the unilateral measures in the IP context, namely by the “special 301” review.

---

Now, that we have established that there are cases of laws with extraterritorial effects both within EU and other national laws (US), the next step, in our analysis, is to explore whether these privacy laws are compatible with the WTO Rules.

The compatibility of such laws with WTO rules has been raised before and solved by the WTO Dispute Settlement Body and then Appellate Body in a decision concerning the US legislation on Internet Gambling\footnote{WTO, Appellate Body Report, USA-Measures affecting the Cross Border Supply of Gambling and Betting Services, WT/DS285/AB/R, 7 April 2005, available at: http://www.wto.org/english/tratop_E/dispu_e/285abr_e.doc}. The Dispute Settlement Body of the W.T.O. in a first moment and the Appellate Body in a second time were requested to solve the dispute between the “Antigua” and the US concerning the limitations created by the US Wire Act upon cross-border provisions of the Internet Gambling and betting services. The “public morals” exception was invoked by the US. The WTO Appellate Body opinion followed a “two-tier analysis”\footnote{WTO, Appellate Body Report, USA-Measures, supra note 455, p. 98.}: First, analyzed and found that, the Wire Act effects directly the cross-border supply of gambling services through the internet. Second, analyzed whether the measure (i.e., the US Wire act) is acceptable under paragraphs “a” and “c” of the Article XIV of the GATS, that is, whether the measure is “necessary” to protect the “public morals” or to maintain the “public order”.

The WTO Appellate Body considered as “vital and important at the highest degree”\footnote{WTO, Appellate Body Report, USA-Measures, supra note 455, p. point 301.} the adoption of the Wire Act. The Appellate Body found that the measure was “necessary”, and therefore justified, under chapeau of Article XIV.

The same arguments might be applied to the compatibility of the Directive 2002/58/EC with the WTO rules\footnote{POULLET, supra note 41, p. 14.} as well as to the eventual extension of the extraterritoriality of the Directive 95/46/EC.

A part from the reasoning held by the WTO judges in this gambling case, one might conclude that, despite its extraterritorial impact or dimension and its effects on the free cross-border market, the extraterritorial scope of application of the Directive 2002/58/EC would be considered as not infringing the WTO rules\footnote{POULLET, supra note 41, p. 14.}. In order to demonstrate that conclusion, we will analyze the EU privacy rules under the “two-tier analysis” followed by the WTO Appellate Body in the US Wire Act case.

First of all we should analyze whether, privacy falls under the exceptions in the meaning of the Article XIV of the GATS. In fact Privacy is expressly mentioned in the Article XIV of the GATS as a possible exception to this free cross-border market, if no arbitrary or unjustified discrimination exists. Moreover, the WTO preamble highlights the importance “of giving due respect to national policy objectives”. At this respect nobody would contest that the privacy and data protection is considered by the EU and its Member States Constitutions as a human right and its protection is deemed as a “public order” and as previously said under the European Court of Human Rights case-law, it is the absolute duty of the EU Member States to ensure this right effectively in the new ICT context and to give absolute priority to the ECHR rules vis-à-vis any other rule, including international commitments and conventions like WTO. Based on these arguments one can conclude that the protection of the privacy in the EU is deemed to be a “public order”.

Having said that, it remains to check if the EU measures respect the “necessary” requirement of the WTO rules. PEREZ-ASINARI, has proposed a “four-steps-methodology” in applying the exceptions of privacy and public order\textsuperscript{460}.

The extraterritorial scope of the 2002/58 Directive is justified by the necessity of taking into consideration the characteristics of the global and interactive Internet network. Insofar these characteristics multiply the possibility of privacy threats by trans-border and uncontrollable Data flows, the EU position and its adoption of certain restrictive measures might be deemed as “necessary” even if they are effecting the cross-border supply of the Internet services.

No possible discrimination will exist insofar the EU authorities might intervene towards any infringing service supplier wherever he is located. It might be underlined that no prior authorization for the supply of electronic communication services is required, what would have created major concerns about the proportionality of this regulatory system and would have been judged as discriminatory by giving privileges to the EU suppliers. The obligation imposed to every supplier and the \textit{a posteriori} intervention, even if they have impact on the cross-border trade ought to be considered as necessary to secure compliance with the EU requirements and create no risks of discriminatory application between countries\textsuperscript{461}.

Using the same arguments the extension of the extraterritorial effect of the Directive 95/46/EC would not infringe the WTO rules.

\textsuperscript{460} M.V. PEREZ-ASINARI, “The WTO and the Protection of the Personal Data. Do EU Measures fall within the GATS Exception? Which future for data protection within the WTO e-commerce Context?” 18\textsuperscript{th} BILETA Conference: Controlling information in the Online Environment within the WTO Rules” 9 Electronic Communications Law review, 2002, 249-280, quoted by POULLET, supra note 41, p. 15.

\textsuperscript{461} POULLET, supra note 41, p. 15.
In that context one might not deny that the European Union is committed and has the obligation, according to the EU treaties to ensure its residents’ privacy and data protection as an element of its fundamental human right values. This defense might not be ensured as it was the case before the expansion of the Internet, which means in the context of the adoption of the Directive 95/46/EC, by controlling certain TBDF mostly identifiable. Experienced in the very disparate contexts of our daily life, the progressive invasion in our life and in our terminals by the worldwide and ubiquitous internet technology requires from the European authorities new regulatory measures which will be applied notwithstanding the location of the intruder\textsuperscript{462}. This would require amending the Directive 95/46/EC in order to extend its extraterritorial effect. The adoption of these new measures and their application must fully take into account the legitimate limitations imposed by the rules of the international trade, in the same manner this international trade might not alleviate the rules dictated by the public order objectives pursued by the EU authorities in protecting privacy\textsuperscript{463}.

To sum this section up, one can argue that claiming extraterritoriality of the Data Protection Law, notably Directive 95/46/EC is a viable solution under the EU privacy Law and compatible with the International Law (WTO rules).

Of course, the extraterritorial solution would not be an ideal solution, nor does it substitute the need for finding global solution to privacy norms, but it is increasingly important that the EU privacy laws begins to think “outside the box”, if we are not to be drowned by a tidal wave that would make the “tide” of community law, that Lord Denning complained of appear as no more than a ripple on the transatlantic pond in comparison\textsuperscript{464}.

\textsuperscript{462} POULLET, supra note 41, p. 16.
\textsuperscript{463} POULLET, supra note 41, p. 16.
\textsuperscript{464} REID, supra note 60, p.502.
9 Conclusions and recommendations

“Without an innovative renewal of data protection law freedom
will diminish in such an unnoticed way as clean water and air have”

Sólyom 1988

9.1 Conclusions

The privacy and data protection has risen sharply up the political and public agenda. This high profile time for privacy and data protection has a paradoxical aspect as far as the research in the subject is concerned. On the one hand, the increased interest for research and knowledge in this field of law encourages many scholars and commentators to carry out research and to contribute in the deepening and widening of the stock of the knowledge in the field. On the other hand, the fact that data protection is a fluid and ever moving subject discourages many scholars and lead them to abandon the subject waiting for a moment when things were more stable.

However, waiting for more stable moments in this subject, it is probably in vain, given that data protection is being developed so rapidly and changed in so many ways. Moreover, it is widely acknowledged that the regulation of the data processing and data flows is destined to remain one of the most important regulatory and policy issues of the 21st century. On that recognition, the author of this thesis decided to carry out research and to write this thesis on data protection law hoping to make a contribution, however small, to the wider debate on the data protection in general and to the EU data protection in particular.

The primary objective of this thesis was to analyze the recent developments of the data protection law with a particular focus on the European Data Protection Law, notably the Directive 95/46/EC.

The research showed that the right to data protection emerged as a legal response to the threat posed to the privacy and identity of the individuals by the mass processing of the information. It emerged as a new legal field in the early 1970s, separate from the privacy law but dependent upon it. The development of the computer technology in the sixties and seventies and the power of the early big mainframe computers made the civil libertarians worry. The new field followed the growth of the information technologies and globalization
processes. Ever since the evolution of the data protection law underwent several stages corresponding to new privacy challenges.

Today, the concern about the privacy and data protection remains largely the same as before. Information is power. Every organization both in private and public sector uses personal information. Every one of us has information about ourselves which is stored somewhere and used by others. On the one hand, there is a very real need to facilitate the use of personal data by all organizations. Personal data is of considerable commercial value to many organizations, whilst for others they need to hold and process personal data to perform their activities and obligations effectively. Health care providers need to keep data about their patients or clients so that they can deliver appropriate and effective treatment and general health care. Thus processing of personal data is beneficial to us to have services in a more efficient way.

On the other hand, there are significant dangers related to the processing personal data. The dangers for individuals related to personal data can present themselves in different ways. The principal dangers that the processing of personal information cause for individuals is that information about them are:

- Inaccurate, insufficient or out of date,
- Excessive or irrelevant,
- Kept for too long,
- Disclosed to those who ought not to have it,
- Used in unacceptable or unexpected ways beyond their control, or,
- Not kept securely.

These risks are not only hypothetical, but, unfortunately, there are also true stories of the consequences that inaccurate personal information can have for the individuals. In UK a man of good character without any criminal conviction was arrested and charged with driving whilst disqualified because incorrect information was stored against his name on the police national computer. The information has been entered against his name by mistake. As a consequence of this, he lost his job and had his car impounded. It took to him four months to trace the man to whom the conviction related and who had a very similar name, before he could clear his name. Besides the immediate personal harm, the processing of data can also cause societal harm such as the loss of personal autonomy or dignity, arbitrary decision-
making about individuals, their stigmatizations or exclusions as well as the growth of excessive organizational power.

**Therefore, while we all have substantial interest in processing our data to receive services in an efficient way, this processing has its dangers. This is an eternal tension.** The task of the personal data law is to provide a legal framework which is capable of reconciling the needs and interests of those who make use of personal data with those of persons to whom these data relate. Too little control and the opportunities for abuse prejudicing the rights and the individuals are manifold. Too much control and the operations of organizations, whether in the public or private sector, will be seriously hampered by the excessive bureaucracy and the interference by bodies administering this important area of law. The solution is that data protection law struck a reasonable balance between these conflicting interests.

**Europe has proven to be the leader in protecting privacy and personal data. The world’s first data protection law was adopted in Europe in (in 1970 in the German Land of Hesse).** In addition to the technological factors, determinative for the emergence of the data protection laws in Europe were also ideological, philosophical and historical factors. Concerns of privacy tend to be high in societies espousing liberal ideals. The development of legal regimes for privacy protection is most comprehensive in the western democracies (i.e. EU and USA). By contrast such regimes are under-developed in most African and Asian nations. However, in the USA—often portrayed as the citadel of the liberal ideals—the legal respect for privacy falls short in significant respects of the protection levels offered by the EU. European law has recognized that data is important per se. This approach is in stark deference with the American approach. These differences derive from the fact that the value placed upon privacy in the US and EU varies considerably from each-other. In the US the data protection is a sub-category of the right to privacy, understood in the background of liberty and of free flow of information. The European privacy law protects dignity, while American privacy law protects liberty. However, this variation between the US and Europe, can be attributable - at least in part- to differences in perceptions of the degree to which privacy is or will be threatened. The comprehensive data protection framework in Europe undoubtedly reflects the traumas from the experience of totalitarian oppressions (i.e. Nazism and Communism).

**Current data protection for the Europeans is afforded by two horizontal legal instruments: the Data Protection Directive 95/46/EC in the framework of the first pillar and the Council Framework Decision 2008/977/JHA in the framework of third pillar.**
Directive 95/46/EC was passed in 1995 to harmonize national data protection laws within the European Community, with the aim of protecting the fundamental rights and freedoms of individuals including their privacy and personal data. Directive 95/46/EC is the first regional legislation in the world to deal with the protection of the privacy. It is also the first piece of legislation in the Union to deal directly with human rights. Also the Directive 95/46/EC is also seen as a unique form of soft legal globalization. The data protection laws of other countries and regions are modeled after the EU Directive, which is acknowledged as the main engine of an emerging global legal regime on data protection. Thus, knowledge of how the data protection is regulated in Europe is useful in predicting how other regions may deal with the subject as well.

The legal research question raised at the beginning of this research was whether the Data Protection Directive 95/46/EC fit the objectives for which it was adopted in 1995. The starting point of the research was the evaluation of the European Commission stance about the Directive. European Commission considers that the Directive 95/46/EC fulfils its original objectives and therefore does not need to be amended.

However, the research carried out for this thesis questioned this static approach of the European Commission to the data protection regime and argued that the Directive does not fit the purposes for which it was adopted 15 years ago.

**The thesis analyzed the legal issues that arise under the Directive 95/46/EC against the wider technical and legal backgrounds and revealed many legal problems and weaknesses.** When the directive was adopted, 15 years ago, the intention was not to create a legal framework, which was well adjusted to take on future data protection and privacy challenges, but, rather to harmonize the existing regulations and to create a common European market for the free movement of personal data. The fluidity of the personal data collections has increased to a point that could not have been imagined at the time of the adoption of the Directive. The increasing pressure on privacy due to the development of privacy destroying technologies and the growing use of and demand for personal information by public and private sectors, requires quick legal answer and constant change of the EU data protection legislation. It is thus clear that the context in which the Data Protection Directive was created has changed fundamentally and certain basic assumptions of the directive have already been challenged.

Against this background, various stakeholders (EDPS (2007), European Privacy and Data Protection Commissioner’s Conference (2009), UK Informational Commissioners (ICO
think-tank (Rand Europe) and commentators believe that the European Data Protection law needs to be reviewed and modernized in order to meet the technological and social challenges of the 21st century.

**Among others three are the main challenges that the EU data protection will face: first the theoretical-political challenge, the legal challenge and the technological challenge.** Since privacy is understood differently in the EU, US, APEC and elsewhere, the main challenge for the privacy is to construct a global data protection regime, which can be achieved either by choosing the best understanding of privacy, or by harmonizing the current privacy concepts. The competition to choose the best understanding of privacy is a tough one mainly between the EU and the US as the two titans of privacy frameworks. The analysis showed that it is extremely doubtful that we will see, at least in the short term, major progress with respect to harmonization at the global level. From the EU data protection point of view, remains two other solutions: first, the regional harmonization, that is, to bring the data privacy regimes of non-EU countries in line with its preferred model. The second solution is the extraterritoriality that is, extending the Extraterritoriality of the EU data protection rules, even though it would remain politically controversial and would raise the problem of enforceability of the decisions.

**As far as the technological challenge is concerned, the** dangers are set to increase since the computer technology becomes progressively more powerful. Therefore the challenge for EU law-makers is to adopt laws to keep pace with the advances in rapidly changing circumstances.

**To meet the external challenges the EU needs first to win its internal challenge.** Accordingly, there is the need, to start the debate on the review of the Directive 95/46/EC. Of course there are no panacea, because the interest protected by privacy and data protection laws is inherently in conflict with other legitimate interests (freedom of speech, public security, free flow of information), but, the new challenges posed to the privacy by public bodies and private organizations, the new privacy-destroying technologies will have to be met with a legal and social response, that is at least as subtle and multifaceted as the technological challenge. Given the rapid pace at which privacy-destroying technologies are being invented and deployed, a legal response must come soon, or it will indeed be too late.

Furthermore, the review the Directive 95/46/EC presents a clear opportunity for Europe to take the lead on privacy protection and once again, as was done with the original Directive, at the time, establish a reference model for many years to come.
9.2 Recommendations

Using the results of the previous chapters as an analytical platform now we come to the last section of this thesis which considers the questions of what changes to the EU data protection law might improve the current situation. Based on the research carried out for this thesis and the relevant analysis, the author believes that the principles underpinning the Directive 95/46/EC are sound, but changes are necessary to clarify the legal framework governing the data protection at the EU level. In order to address the main issues discussed above, it is recommended that a number of quite different measures be considered.

These measures recommended are first, essential aspects which can be dealt with only by amending the text of certain provisions of the Directive 95/46/EC or by adding further Articles and second, aspects which are advisable but not essential. What is recommended is not a radical change of the EU data protection law but an improvement of some of its weaknesses and shortfalls. The recommendations are the following:

9.2.1 Recommendations of essential importance

1. Consideration should be given to adopt a comprehensive legal framework on data protection, applicable across different activities of the Union.

Rationale:

In favour of this approach are many arguments. First, as we analyzed above the current stipulations on the Directive (for the first pillar) and the Framework Decision (for the third pillar) are not natural or very practical ones, because the boundary between matters within and without the scope of Community Law is unclear, and what is more the boundary is also continually shifting. Second, from the point of view of the Member States, it would be easier to apply in the national law a single legal instrument than two legal instruments which creates problematic and unwarranted “seams” between data protection regimes in different (but not easy to separate) sectors. Third, the laws of all the Member States which have implemented the Directive, apply, in principle, “across the board”, to matters both within and without the scope of Community law - even though they also often contain quite sweeping exemptions and exceptions concerning typical “Third Pillar” matters such as
police or state security matters\textsuperscript{465}. Therefore, a single instrument would overcome the problems arising from the uncritical application by the member states of some provisions in the Directive, related to data processing in matters outside the scope of Community law.

Forth, the Treaty of Lisbon opens up for a genuine comprehensive data protection framework. The Treaty, first, ends the pillar structure of the Union and second, the new Article 16 (TFEU) provides for the necessary legal basis for one comprehensive legal framework applicable across different activities of the Union.

This new legal framework would enhance the consistency of the system, ensures legal certainty, improve the protection of the data subjects and in particular, would avoid in the future the difficulties of finding a dividing line between the pillars or the legal basis of EU instruments adopted in the field of data protection.

2. The Directive should be a human rights instrument.

Rationale:

Given that the data protection law originated as a legal reaction to the threats posed to privacy by technological developments, the \textit{raison d’être} of the Directive should be the protection of the right to data protection and all other competing interest (i.e. market, security considerations) should be subordinated to this right. Accordingly, the provisions of the Directive, emphasizing that the data protection is a fundamental right should be amended to refer to Article 16 of the Treaty of Lisbon and to Article 8 of the Charter of Fundamental Rights and use the terminology of these two instruments.

3. The Directive should lay down special provisions for the protection of personal data of the children.

Rationale:

Directive 95/46/EC apply to all natural persons (i.e. including children), but there are no specific provisions relating to issues particular to children\textsuperscript{466}. This is necessary because of the new threats posed to them by the new technologies and due to the fact that the young

\textsuperscript{465} KORFF, \textit{supra note} 98, p. 42.

people had never been so measured, graded and monitored\textsuperscript{467}. Therefore it is recommended to introduce provisions in the directive to ensure that children privacy is adequately protected.

4. **The directive should define the term “transfer of personal data” (Article 2).**

**Rationale:**

The concept of “transfer of personal data” is important both for the transfer of data within the EU and notably, in determining whether restrictions under EU law on transferring personal data to third countries are applicable. Moreover, since the data protection law of many Member States (e.g. Germany) defines this concept, it would be necessary to have a harmonized legal concept at the EU level.

5. **Recommendations for the “Applicable law” Article 4.**

In order to address the problematic aspects of the Article 4 of the Directive, the “applicable law” rules laid down in that article need to be re-drafted in such a way as to remove ambiguities in the present text, and will then have to be implemented identically in the Member States, if one of the main purposes of the Directive is not to be defeated\textsuperscript{468}.

5.1. **The “Applicable law rules” laid down in Article 4(1)(a) that seek to ensure that within the EU only one law applies to anyone processing operation (within the scope of the Directive) must be simplified and then uniformly applied.**

**Rationale:**

Concerning the problem of the data subjects having to cope with the foreign legal systems, to remedy this problem we recommend that: the applicable law should not be the law of the Member State, where the controller is established, but the law of the state in which the data subject has its domicile. This solution would be similar to the rules of the European Private International Law\textsuperscript{469} for the choice of law in the case of consumer contracts. This would in

\textsuperscript{467}WARREN, “The end of privacy?”, the Guardian, Thursday 2 April 2009, available at: www.guardian.co.uk.

\textsuperscript{468}KORFF, supra note 98, p.48.

\textsuperscript{469}See the 1980 Rome Convention on the Law Applicable to contractual obligations, Article 5, (Certain consumer Contracts); and the 2008 Regulation on the Law Applicable to the Contractual Obligations (Rome I), Article 6 (Consumer Contracts), O.J.L. 177/6.
conformity with the general philosophy underpinning the data protection laws which are designed to protect the data subject as the weak part in a data processing operation.

5.2. The “applicable law” rules laid down in Article 4(1)(c) needs to be re-drafted to clarify the position of the non-EU based controllers.\footnote{KORFF, supra note 98, p.247.}

_Rationale:_

The “applicable law” provisions of the Directive (Article 4(1)(c)), must be revised to make it possible for the non-EU based controllers to apply one law to cross-border operations within the EU, on a par with the EU based controllers, as far as there is a clearly identifiable person or organization who or which can be held responsible for the processing\footnote{KORFF, supra note 98, p.247.}. The possibility of the “regulatory overarching” could be reduced, if the Article 4(1)(c) is limited to two situations:

- Where the controller attempts to circumvent the law of an EU Member State by relocating his establishment to a third country (but still uses means situated in the EU),
- Where the controller himself (who is located in the third country) transmits data to a third country for further processing (again using means situated in Europe).\footnote{BYGRAVE (2000), supra note 279, p.10.}

6. Article 9 of the Directive needs to be rephrased in order to better reconcile data protection with freedom of expression and freedom of information.

_Rationale:_

Article 9 of the Directive is somewhat at odd with other European Instruments (Article 10 of the ECHR and Article 11 of the EU Charter of Fundamental Rights) which protect the freedom of expression for “everyone”. The Directive does not recognize the freedom of expression to everyone, but through special derogations only for the benefit of “processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression”. This can only be remedied by amending the text of Article 9 of the Directive in such a way as to formally recognize the (constitutional) need to provide for

\footnote{KORFF, supra note 98, p.247.}
\footnote{KORFF, supra note 98, p.247.}
\footnote{BYGRAVE (2000), supra note 279, p.10.}
derogations from the rules in the Directive whenever the right to freedom of expression of anyone would be unduly affected by the unmitigated application of those rules.\(^\text{473}\)

5. The Directive should lay down the right of the data subjects to access the most public services anonymously

**Rationale:**

Some public services are still anonymous (bus ticket), others need names (criminal records). The big question is what happens in the middle. The key is the right to anonymity. We believe that most public-sector systems should offer anonymous service to those who need or want it. This recommendation serves at least two functions: First, it helps to deter departments from building empires around unnecessary personal information and second, it sets out to minimize discrimination in service provision.\(^\text{474}\) An explicit right to anonymity will not only restore an ancient right, but also poison future governments’ attempts to hedge in citizens’ freedoms.\(^\text{475}\)

6. Insertion of a new provision after Article 25 to govern the intra-community data transfers to matters not subject to the Directive.

**Rationale:**

The transfer of personal data to other Member States of the EU, in relation to matters not subject to the Directive, should be subject to the same approach as it is adopted with regard to transfers to “third countries”. A new Article needs to be inserted after Article 25.\(^\text{476}\)

The freedom to transfer personal data to other EU Member States, stipulated by the Directive, should be **limited to matters within the scope of the Directive**. Transfers of personal data to the other Member States in connection with matters not within the scope of the Directive (Article 3(2)) should be subject to the same approach as it is adopted with regard to transfers to “third countries”, i.e. they should be allowed if it has been formally determined that “adequate” (or indeed, given that data protection is included in the Charter, “equivalent”) protection is ensured in respect of the processing of the data in the non-

\(^{473}\)KORFF, supra note 98, p.206.


\(^{475}\)Ibid. p. 44.

\(^{476}\)KORFF, supra note 98, p.248.
Community context in the other Member State, or if certain special derogations apply (which should be subject to appropriate safeguards).\textsuperscript{477} Therefore, any revision of the Directive should ensure that its provisions are not applied by the Member States in such a way as to deprive their citizens of their fundamental rights under national or European law.

### 9.2.2 Recommendations that are advisable but not essential

7. \textit{The directive should spell out more precisely how certain very important provisions of the Directive must be transposed into the laws of the Member States.} This is important with regard to\textsuperscript{478}:

- the definitions of the directive (Article 2) which should be repeated \textit{verbatim} in the laws of the MS,

- the rules of the applicable law (Article 4), which must be uniformly transposed in the laws of the Member States.

- the status of the national laws giving effect to the Directive in the national law system which should be such as to adopt a rule – in line with the Greek or Danish laws - according to which, the laws which give effect to the Directive prevail over other national laws in matters of data protection, at least as concerns processing relating to activities within the scope of Community law.

\textbf{Rationale:}

The way in which the Directive is transposed into national law must be left to the Member States. However, very divergent ways in which the Member States have given effect to the above matters (or have failed to do so) created major obstacles to the Internal Market. Clear and binding stipulations on at least the above matters are therefore, crucial to the removal of such obstacles\textsuperscript{479}.

8. \textit{The Directive should follow a combined approach, that is, the simplification of some Articles of the Directive coupled with measures allowing for binding clarifications and

\textsuperscript{477} KORFF, supra note 98, p. 174.
\textsuperscript{478} KORFF, supra note 98, p. 249.
\textsuperscript{479} KORFF, supra note 98, p. 249.
more detailed determinations for some selected matters. Matters that should be simplified in the directive include:

- Definitions in Article 2 (from which the gloss could be removed and moved to a subsidiary guidance, in which further matters are also clarified),

- Rules on further processing or prolonged retention of data for research purposes, contained in the second sentence of Arts. 6(1)(b) and 6(1)(e), (which can be moved to such subsidiary guidance altogether, which would also allow for clarification of what kinds of safeguards are “appropriate” in this context),

- Examples of the further information which have to be given under Articles 10 and 11 in order to ensure fair processing (which again can be moved to such guidance and then expanded on).

Rationale:

Such a combined approach would allow for the application of the Directive in accordance with the “risk-related” \ “prevention of misuse” approach advocated by several Governments and other parties and, more importantly, would result in a more uniform (less divergent) yet still flexible application of the Directive in specific contexts\(^{480}\).

If various clarifications which are currently contained in the text of the Directive (in particular, in the definitions) are removed, a general subsidiary guidance should be issued with the amended Directive re-stating those clarifications (and adding to them).

If the above approach is adopted, and the possibility of issuing of subsidiary clarification or guidance is created in the Directive, the procedure for the issuing of such subsidiary clarification or guidance must be clarified. It is recommended that the “Comitology” provided for in Art. 31(2) - and which is already used in important matters relating to cross-border transfers - would be appropriate in principle.

\(^{480}\) KORFF, supra note 98, p. 249.
Bibliography

I. BOOKS


II. DOCUMENTS OF EUROPEAN INSTITUTIONS

EUROPEAN COMMISSION


Communication from the Commission to the Council and the European Parliament on *Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM (2007), 228 final, 2.5. 2007.


Proposal for Council Framework Decision on the on the Use of the Passenger Name Records (PNR) for Law enforcement purposes (COM 2007) 654.


EUROPEAN PARLIAMENT


COUNCIL OF THE EUROPEAN UNION:


COUNCIL OF MINISTERS:


III. DOCUMENTS OF EU MEMBER STATES


Draft Resolution by the French Senate regarding the Nomination by the European Commission of an Group of Experts on Data Protection, Senate Ordinary Session of 2008-2009, Setting of 6 February 2009, available at the website:
http://www.senat.fr/leg/ppr08-203.html

IV. INTERNATIONAL INSTRUMENTS AND ACTS


V. LEGISLATIVE INSTRUMENTS AND INTERNATIONAL AGREEMENTS


EU-USA Agreement on the processing and transfer of passengers name record (PNR) data by Air carriers to the United States Department of Homeland Security, signed on 23 July 2007 by the EU (OJ L 204, 4.8.2007, p.18).
The Treaty of Prüm was signed on 27 May 2005 by the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria, Council Document 10900/05, 7 July 2005.

VI. CASE-LAW OF THE ECJ, CFI, OF ECtHR AND OF W.T.O. DISPUTE SETTLEMENT BODY

CASE-LAW OF THE ECJ AND OF CFI

Case C-101/01, Criminal Proceedings against Bodil Lindqvist, [2003], ECR I-12971.
Case C-275/06, Productores de Musica de Espana (Promusicae) v Telefonica de Espagna SAU, [2008] E.C.R. I-0271
Case C-301/06, Ireland v Parliament and the Council, Judgment of 10 February 2009, not yet reported.
Case C-524/06, Heinz Huber v Bundesrepublik Deutschland [2008], Judgment of 16 December 2008, not yet reported.
Case C-553/07, College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, Judgment of 7 May 2009, not yet reported.
Case C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, Order of the Court of 19 February 2009, not yet reported.
Case C-73/07, Tietosuojaavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, Judgment of 16 December 2008, not yet reported.
Case T-102/96, Gencor Ltd v Commission of the European Communities, [1999] ECR. II-753

Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others [2003] ECR I-4989, [2003] ECR I-6041,


CASE-LAW OF THE ECtHR


Case Copland v. The United Kingdom, (Application no. 62617/00), Judgment of 3 April 2007.


Case Tyrer v. UK, (Application no. 5856/72), Judgment of 25 April 1978,


OPINIONS OF THE ADVOCATES GENERALS:


WTO DISPUTE SETTLEMENT BODY


VII. OPINIONS AND OTHER ACTS OF EUROPEAN DATA PROTECTION SUPERVISOR


Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (2008/C 110/01), point 25.


**VIII. OPINIONS AND OTHER ACTS OF ARTICLE 29 WORKING PARTY**

11th Annual Report of the Article 29 Working Party on Data protection: on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2007, of 24.06.2008,


IX. PAPERS


X. PRESS ARTICLES


WRAY, R., “Phorm: UK faces court for failing to enforce EU Privacy laws”, guardian.co.uk, Tuesday, 14 April, 2009.


XI. REPORTS


XII. REVIEWS


ANNEX
## ANNEX I: Data protection laws worldwide

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Countries</th>
<th>OECD</th>
<th>CoE</th>
<th>EU Members</th>
<th>EU Adequate</th>
<th>Under EU Assessment/Ne gotiations</th>
<th>APEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Albania</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Argentina</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Andorra</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Armenia</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Australia</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Austria</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Azerbaijan</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Belgium</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Bosnia and Herzegovina</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Brunei Darussalam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Bulgaria</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Canada</td>
<td>+</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Chile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>China</td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Croatia</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Cyprus</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Czech Republic</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Denmark</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Estonia</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Faroe Island</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Finland</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>France</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>----------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Georgia</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Germany</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Greece</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Hong Kong</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Guernsey</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Hungary</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Iceland</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>India</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Indonesia</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Ireland</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Isle of Mann</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Israel</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Italy</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Japan</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Jersey</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Korea Republic</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Latvia</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Liechtenstein</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Lithuania</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Luxembourg</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Malaysia</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Malta</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Mexico</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Moldova</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Monaco</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Montenegro</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>----------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>49</td>
<td>Netherlands</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>New Zealand</td>
<td>+</td>
<td></td>
<td></td>
<td>+</td>
<td>[negotiations]</td>
<td>+</td>
</tr>
<tr>
<td>51</td>
<td>Norway</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Papua</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Poland</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Portugal</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Peru</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Philippines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Romania</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Russia</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>San Marino</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Serbia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Singapore</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Slovakia</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Slovenia</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Spain</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Sweden</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>Switzerland</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Taipei</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Thailand</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>FYROM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>Turkey</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>Ukraine</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>United Kingdom</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>United States</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>Vietnam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ANNEX II: 2007 Agreement between the EU and US on the processing and transfer of passenger name record (PNR) data by air carriers to the US Department of Homeland Security (DHS)⁴⁸¹

THE EUROPEAN UNION

and

THE UNITED STATES OF AMERICA,

DESIRING to prevent and combat terrorism and transnational crime effectively as a means of protecting their respective democratic societies and common values.

RECOGNISING that information sharing is an essential component in the fight against terrorism and transnational crime and that in this context the use of PNR data is an important tool.

RECOGNISING that, in order to safeguard public security and for law enforcement purposes, rules should be laid down on the transfer of PNR data by air carriers to DHS.

RECOGNISING the importance of preventing and combating terrorism and related crimes, and other serious crimes that are transnational in nature, including organized crime, while respecting fundamental rights and freedoms, notably privacy.

RECOGNISING that U.S. and European privacy law and policy share a common basis and that any differences in the implementation of these principles should not present an obstacle to cooperation between the U.S. and the European Union (EU).

HAVING REGARD to international conventions, U.S. statutes, and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to make PNR data available to DHS to the extent they are collected and contained in the air carrier's automated reservation/departure control systems (hereinafter "reservation systems"), and comparable requirements implemented in the EU.

HAVING REGARD to Article 6 paragraph 2 of the Treaty on European Union on respect for fundamental rights, and in particular to the related right to the protection of personal data.

NOTING the former agreements regarding PNR between the European Community and the United States of America of 28 May 2004 and between the European Union and the United States of America of 19 October 2006.


NOTING that the European Union should ensure that air carriers with reservation systems located within the European Union make available PNR data to DHS and comply with the technical requirements for such transfers as detailed by DHS.

AFFIRMING that this Agreement does not constitute a precedent for any future discussions or negotiations between the United States and the European Union, or between either of the Parties and any State regarding the processing and transfer of PNR or any other form of data.

SEEKING to enhance and encourage cooperation between the parties in the spirit of transatlantic partnership,

HAVE AGREED AS FOLLOWS:

(1) On the basis of the assurances in DHS's letter explaining its safeguarding of PNR (the DHS letter), the European Union will ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America will make available PNR data contained in their reservation systems as required by DHS.

(2) DHS will immediately transition to a push system for the transmission of data by such air carriers no later than January 1, 2008 for all such air carriers that have implemented such a system that complies with DHS's technical requirements. For those air carriers that do not implement such a system, the current systems shall remain in effect until the carriers have implemented a system that complies with DHS's technical requirements. Accordingly, DHS will electronically access the PNR from air carriers' reservation systems located within the territory of the Member States of the European Union until there is a satisfactory system in place allowing for the transmission of such data by the air carriers.
(3) DHS shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable U.S. laws, constitutional requirements, and without unlawful discrimination, in particular on the basis of nationality and country of residence. DHS’s letter sets forth these and other safeguards.

(4) DHS and the EU will periodically review the implementation of this Agreement, the DHS letter, and U.S. and EU PNR policies and practices with a view to mutually assuring the effective operation and privacy protection of their systems.

(5) By this Agreement, DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory resolution. In the event that a PNR system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for persons whose travel itinerary includes a flight to or from the European Union, DHS shall, strictly on the basis of reciprocity, actively promote the cooperation of the airlines within its jurisdiction.

(6) For the application of this Agreement, DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union. Concomitantly, the EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds.

(7) The U.S. and the EU will work with interested parties in the aviation industry to promote greater visibility for notices describing PNR systems (including redress and collection practices) to the travelling public and will encourage airlines to reference and incorporate these notices in the official contract of carriage.

(8) The exclusive remedy if the EU determines that the U.S. has breached this Agreement is the termination of this Agreement and the revocation of the adequacy determination referenced in paragraph (6). The exclusive remedy if the U.S. determines that the EU has breached this agreement is the termination of this Agreement and the revocation of the DHS letter.
(9) This Agreement will enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose. This Agreement will apply provisionally as of the date of signature. Either Party may terminate or suspend this Agreement at any time by notification through diplomatic channels. Termination will take effect thirty (30) days from the date of notification thereof to the other Party unless either Party deems a shorter notice period essential for its national security or homeland security interests. This Agreement and any obligations there under will expire and cease to have effect seven years after the date of signature unless the parties mutually agree to replace it.

This Agreement is not intended to derogate from or amend the laws of the United States of America or the European Union or its Member States. This Agreement does not create or confer any right or benefit on any other person or entity, private or public.

This Agreement shall be drawn up in duplicate in the English language. It shall also be drawn up in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish languages, and the Parties shall approve these language versions. Once approved, the versions in these languages shall be equally authentic.

Done at Brussels on 2007 and at Washington on 2007

FOR THE UNITED STATES OF AMERICA FOR THE EUROPEAN UNION

U.S. Letter to EU

Salutation,

In response to the inquiry of the European Union and to reiterate the importance that the United States government places on the protection of individual privacy, this letter is intended to explain how the United States Department of Homeland Security (DHS) handles the collection, use and storage of Passenger Name Records (PNR). None of the policies articulated herein create or confer any right or benefit on any person or party, private or
public, nor any remedy other than that specified in the Agreement between the EU and the U.S. on the processing and transfer of PNR by air carriers to DHS signed in … 2007 (the "Agreement"). Instead, this letter provides the assurances and reflects the policies which DHS applies to PNR data derived from flights between the U.S. and European Union (EU PNR) under U.S. law.

I. Purpose for which PNR is used:

DHS uses EU PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law. DHS will advise the EU regarding the passage of any U.S. legislation which materially affects the statements made in this letter.

II. Sharing of PNR:

DHS shares EU PNR data only for the purposes named in Article I.

DHS treats EU PNR data as sensitive and confidential in accordance with U.S. laws and, at its discretion, provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and U.S. law on the exchange of information between U.S. government authorities. Access shall be strictly and carefully limited to the cases described above in proportion to the nature of the case.

EU PNR data is only exchanged with other government authorities in third countries after consideration of the recipient's intended use(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understandings between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS, as described in the second paragraph of this article.

III. Types of Information Collected:

Most data elements contained in PNR data can be obtained by DHS upon examining an individual's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically significantly enhances DHS's
ability to focus its resources on high risk concerns, thereby facilitating and safeguarding bona fide travel.

Types of EU PNR Collected:

1. PNR record locator code,
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)
6. Other names on PNR, including number of travelers on PNR
7. All available contact information (including originator information)
8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)
9. Travel itinerary for specific PNR
10. Travel agency/travel agent
11. Code share information
12. Split/divided information
13. Travel status of passenger (including confirmations and check-in status)
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote
15. All Baggage information
16. Seat information, including seat number
17. General remarks including OSI, SSI and SSR information
18. Any collected APIS information
19. All historical changes to the PNR listed in numbers 1 to 18

To the extent that sensitive EU PNR data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual), as specified by the PNR codes and terms which DHS has identified in consultation with the European Commission, are included in the
above types of EU PNR data, DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, as described in the next paragraph, DHS promptly deletes the sensitive EU PNR data.

If necessary in an exceptional case where the life of a data subject or of others could be imperiled or seriously impaired. DHS officials may require and use information in EU PNR other than those listed above, including sensitive data. In that event, DHS will maintain a log of access to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. DHS will provide notice normally within 48 hours to the European Commission (DG JLS) that such data, including sensitive data, has been accessed.

IV. Access and Redress:

DHS has made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S. law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR. These policies are accessible on the DHS website, [www.dhs.gov](http://www.dhs.gov).

Furthermore, PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U. S. Privacy Act and the U. S. Freedom of Information Act (FOIA). FOIA permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA. DHS does not disclose PNR data to the public, except to the data subjects or their agents in accordance with U.S. law. Requests for access to personally identifiable information contained in PNR that was provided by the requestor may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229 (phone: (202) 344-1850 and fax: (202) 344-2791).

In certain exceptional circumstances, DHS may exercise its authority under FOIA to deny or postpone disclosure of all or part of the PNR record to a first part requester, pursuant to Title
Under FOIA any requester has the authority to administratively and judicially challenge DHS's decision to withhold information.

V. Enforcement:

Administrative, civil, and criminal enforcement measures are available under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records. Relevant provisions include but are not limited to Title 18, United States Code, Sections 641 and 1030 and Title 19, Code of Federal Regulations, Section 103.34.

VI. Notice:

DHS has provided information to the travelling public about its processing of PNR data through publications in the Federal Register and on its website. DHS further will provide to airlines a form of notice concerning PNR collection and redress practices to be available for public display. DHS and the EU will work with interested parties in the aviation industry to promote greater visibility of this notice.

VII. Data retention:

DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk. We expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions. Data that is related to a specific case or investigation may be retained in an active database until the case or investigation is archived. It is DHS' intention to review the effect of these retention rules on operations and investigations based on its experience over the next seven years. DHS will discuss the results of this review with the EU.

The above mentioned retention periods also apply to EU PNR data collected on the basis of the Agreements between the EU and the US, of May 28, 2004 and October 19, 2006.

VIII. Transmission:

Given our recent negotiations, you understand that DHS is prepared to move as expeditiously as possible to a "push" system of transmitting PNR from airlines operating flights between the EU and the U.S. to DHS. Thirteen airlines have already adopted this
approach. The responsibility for initiating a transition to "push" rests with the carriers, who must make resources available to migrate their systems and work with DHS to comply with DHS's technical requirements. DHS will immediately transition to such a system for the transmission of data by such air carriers no later than January 1, 2008 for all such air carriers that have implemented a system that complies with all DHS technical requirements. For those air carriers that do not implement such a system the current system shall remain in effect until the air carriers have implemented a system that is compatible with DHS technical requirements for the transmission of PNR data. The transition to a "push" system, however, does not confer on airlines any discretion to decide when, how or what data to push. That decision is conferred on DHS by U.S. law. Under normal circumstances DHS will receive an initial transmission of PNR data 72 hours before a scheduled departure and afterwards will receive updates as necessary to ensure data accuracy. Ensuring that decisions are made based on timely and complete data is among the most essential safeguards for personal data protection and DHS works with individual carriers to build this concept into their push systems. DHS may require PNR prior to 72 hours before the scheduled departure of the flight, when there is an indication that early access is necessary to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with the purposes defined in article I. In exercising this discretion, DHS will act judiciously and with proportionality.

IX. **Reciprocity:**

During our recent negotiations we agreed that DHS expects that it is not being asked to undertake data protection measures in its PNR system that are more stringent than those applied by European authorities for their domestic PNR systems. DHS does not ask European authorities to adopt data protection measures in their PNR systems that are more stringent than those applied by the U.S. for its PNR system. If its expectation is not met, DHS reserves the right to suspend relevant provisions of the DHS letter while conducting consultations with the EU with a view to reaching a prompt and satisfactory resolution. In the event that an airline passenger information system is implemented in the European Union or in one or more of its Member States that requires air carriers to make available to authorities PNR data for persons whose travel itinerary includes a flight between the U.S. and the European Union, DHS intends, strictly on the basis of reciprocity, to actively promote the cooperation of the airlines within its jurisdiction.

In order to foster police and judicial cooperation, DHS will encourage the transfer of analytical information flowing from PNR data by competent US authorities to police and
judicial authorities of the Member States concerned and, where appropriate, to Europol and Eurojust. DHS expects that the EU and its Member States will likewise encourage their competent authorities to provide analytical information flowing from PNR data to DHS and other US authorities concerned.

X. Review:

DHS and the EU will periodically review the implementation of the agreement, this letter, U.S. and EU PNR policies and practices and any instances in which sensitive data was accessed, for the purpose of contributing to the effective operation and privacy protection of our practices for processing PNR. In the review, the EU will be represented by the Commissioner for Justice, Freedom and Security, and DHS will be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate. The EU and DHS will mutually determine the detailed modalities of the reviews.

The U.S. will reciprocally seek information about Member State PNR systems as part of this periodic review, and representatives of Member States maintaining PNR systems will be invited to participate in the discussions.

We trust that this explanation has been helpful to you in understanding how we handle EU PNR data.

---

**EU letter to U.S.**

Salutation,

Thank you very much for your letter to the Council Presidency and the Commission explaining how DHS handles PNR data.

The assurances explained in your letter provided to the European Union allow the European Union to deem, for the purposes of the international agreement signed between the United States and European Union on the processing and transfer of PNR in … on… 2007 that DHS ensures an adequate level of data protection.

Based on this finding, the EU will take all necessary steps to discourage international organizations or third countries from interfering with any transfers of EU PNR to the United States. The EU and its Member States will also encourage their competent authorities to
provide analytical information flowing from PNR data to DHS and other US authorities concerned.

We look forward to working with you and the aviation industry to ensure that passengers are informed about how governments may use their information

Salutary close