Law, Governance and Technology Series 16

Gloria González Fuster

The Emergence of Personal Data Protection as a Fundamental Right of the EU

Springer

The Emergence of Personal Data Protection as a Fundamental Right of the EU

Law, Governance and Technology Series

VOLUME 16

Series Editors:

POMPEU CASANOVAS, *UAB Institute of Law and Technology, Bellaterra, Barcelona, Spain*

GIOVANNI SARTOR, *European University Institute, Florence, Italy*

ISSUES IN PRIVACY AND DATA PROTECTION

Sub Series Editor:

Serge Gutwirth
Law, Science, Technology and Society (LSTS)
Vrije Universiteit Brussels (VUB)
Brussel
Belgium

Scientific Advisory Board:

For further volumes:
http://www.springer.com/series/8808

Gloria González Fuster

The Emergence of Personal Data Protection as a Fundamental Right of the EU

Springer

Gloria González Fuster
Law, Science, Technology and Society
(LSTS)
Vrije Universiteit Brussel (VUB)
Brussels
Belgium

ISSN 2352-1902 ISSN 2352-1910 (electronic)
ISBN 978-3-319-05022-5 ISBN 978-3-319-05023-2 (eBook)
DOI 10.1007/978-3-319-05023-2
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014934169

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To my father, who has taught me how important it is to have the freedom to erase names, and to invent them, and to my mother, who has taught me how important it is to safeguard them.

Acknowledgements

This book is largely based on a Ph.D. thesis defended at the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB) in May 2013. It would not have been possible without the help of Prof. Dr. Serge Gutwirth (main supervisor). For his inestimable knowledge, dedicated support, and exceptional kindness, I consider myself extremely lucky. I am also deeply indebted to Prof. Dr. Paul De Hert (co-supervisor), without whom my academic career would have been significantly less stimulating; to Dr. Antoinette Rouvroy (member of the thesis' Advisory Commission), for her advice and sustained encouragement, and to all the members of the jury for their precious comments and questions: Prof. Dr. Colin Bennett, Prof. Dr. Em. Bart De Schutter, Prof. Dr. Youri Devuyst, Prof. Dr. Mireille Hildebrandt, and Dr. Ricard Martínez Martínez,

I would like to acknowledge the financial support of some projects to which I contributed while carrying out this research: *Reflexive Governance in the Public Interest* (REFGOV), *Converging and conflicting ethical values in the internal/external security in continuum in Europe* (INEX), and *Privacy and Security Mirrors* (PRISMS), all co-funded by the European Union. The collaboration of the staff of the European Parliament's Register of Documents, and at the Historical Archives of the European Commission, was particularly helpful. I also thank VUB's Institute of European Studies (IES), and the Law, Science, Technology and Society (LSTS) Research Group for their kind hospitality. I am thankful to all my colleagues; I cannot mention them all, so I will just mention Rocco Bellanova.

Guillaume De Martelaer encouraged me to undertake this research a long time ago, and has supported me ever since. Our son Jean has been waking me up every morning with a smile. For their help, patience and inspiration, I am profoundly grateful. I am also very much indebted to Josiane and Guy De Martelaer for their affection and availability, and to Daniel González Fuster for his infallible assistance. Thank you.

Contents

Abbreviations

AEPD	Agencia Española de Protección de Datos
AFIPS	American Federation of Information Processing Societies
AFSJ	Area of Freedom, Security and Justice
ASNEF	Asociación Nacional de Establecimientos Financieros de Crédito
BDSG	Bundesdatenschutzgesetz
CDCJ	European Committee on Legal Co-operation
CJ-PD	Project Group on Data Protection
CNIL	Commission nationale de l'informatique et des libertés
DSG	Datenschutzgesetz
EC	European Community
EC Treaty	Treaty establishing the European Community
ECHR	European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms)
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEC	European Economic Community
ESC	Economic and Social Committee
EU	European Union
FECEMD	Federación de Comercio Electrónico y Marketing Directo
FOIA	Freedom of Information Act
FRA	EU Agency for Fundamental Rights
GMD	Gesellschaft für Mathematik und Datenverarbeitung
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Commission of Jurists
INRIA	Institut national de recherche en informatique et en automatique
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
JRC	Joint Research Center
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
MEP	Member of the European Parliament

NCC	National Computing Centre
OECD	Organisation for Economic Cooperation and Development
OJ	Official Journal of the European Union
PETs	Privacy Enhancing Technologies
PNR	Passenger Name Record
RJD	Reports of Judgments and Decisions of the ECtHR
SABAM	Société belge des auteurs compositeurs et éditeurs
SIS	Schengen Information System
T-DP	Consultative Committee (Convention 108)
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
US	United States

Chapter 1
Introduction

Toda palabra llama a otra palabra. ('Every word calls another word' (translated by the author))

(Juarroz 2012)

The book studies the emergence of the right to the protection of personal data as a fundamental right in the law of the European Union (EU). It is the fruit of a double perplexity: it was born of the curiosity roused by the surfacing of a new fundamental right inside the EU legal system, but also of a feeling of puzzlement in face of the persistently limited recognition of the right's advent by the literature, as well as by the judiciary responsible for its interpretation and application,[1] and by those involved in discussing the future of the legal framework supposed to uphold it.

This introductory chapter offers a series of preliminary reflections on the nature of the inquiry. It puts forward the research subject, renders explicit some of the research premises, and describes the research's outline and sources.

1.1 The EU Fundamental Right to the Protection of Personal Data

In December 2000, the European Parliament, the Council and the European Commission solemnly proclaimed in Nice (France) the Charter of Fundamental Rights of the EU (hereafter, 'the Charter').[2] The Charter was the first catalogue of rights ever agreed jointly by the three major EU institutions. It represented the outcome of a decades-long debate on the opportunity of equipping the EU with its own, distinct inventory of rights—different from Council of Europe's 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and from a

[1] Noting how the nature of data protection confuses the literature and courts: (Tzanou 2013, p. 99).

[2] Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law,* Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_1,

mere compilation of the rights set out at national level by EU Member States. The EU Charter formally designates the rights it 'recognises'[3] as 'fundamental rights'.[4]

According to its preamble, the Charter aims 'to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible'.[5] The act of rendering 'more visible' some rights appears to imply that they already existed, even if in a less visible manner. Developing this thought, the Charter's preamble adds that the instrument 'reaffirms'[6] fundamental rights as they result from 'the constitutional traditions and international obligations common to the Member States', as well as from EU primary law, the ECHR, the Social Charters adopted by the Community and the Council of Europe, and the case law of both the Court of Justice of the European Communities[7] and the European Court of Human Rights. If the Charter genuinely 'reaffirms' rights, it might be reasonable to infer that they must have been previously affirmed in any of the mentioned sources.

Article 8 of the EU Charter is titled 'Protection of personal data'. It establishes:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 8 of the Charter thus purportedly asserts the existence of a right to the protection of personal data enjoyed by 'everyone'. The right, however, had not been affirmed before in any of the sources mentioned in the Charter's preamble. If the Charter rendered this right 'more visible', it was essentially because previously it had been invisible. By re-cognising it, the Charter was as a matter of fact acknowledging its birth: creating it. In 2009, the Lisbon Treaty[8] granted legally binding force to the Charter,[9] consolidating the existence in EU law of a (by then visible, or newly created) fundamental right to the protection of personal data.

---

[3] Preamble to the Charter (ibid. 8).

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Named since December 2009 the EU Court of Justice.

[8] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon [2007] OJ C306/1.

[9] In a slightly modified version: Charter of Fundamental Rights of the European Union [2007] OJ C303/1.

The literature has generally regarded the Charter's Article 8 as an innovation,[10] potentially heralding a Copernican turn for personal data protection in Europe (Piñar Mañas 2009, p. 93). But the newness of this novel right has also been nuanced (Bernsdorff 2003, p. 160). It certainly did not emerge ex nihilo; rules applicable to the processing of personal data had materialised in the majority of the sources mentioned in the Charter's preamble (namely, in international obligations common to EU Member States, in EU primary law, and in the case law of the Court of Justice of the European Communities and the European Court of Human Rights), even if differently—not in the shape of a (EU) fundamental right.

The EU right to the protection of personal data has been portrayed as the outcome of a sort of dialogue between legal literature and international, European and national legal systems (Murillo de la Cueva 2009, p. 17), as well as the product of a process or concatenation of actions derived from each other (Coudray 2010, p. 21).[11] This research is directly concerned with examining the pivotal variation in such a dialogue from the absence of a right to its presence, and thus with the question of how could actions that admittedly referred to contrasting realities (the inexistence vs. the existence of a right) fluently interplay with each other, and concatenate.

1.2 Research Questions

The main question of this book is: How did the fundamental right to the protection of personal data surface in EU law, despite the lack of recognition of such a right in any of the sources that formally serve as references for the identification of EU fundamental rights?

Therefore, its central concern is to understand the way in which a specific change (that is, the appearance of the fundamental right to personal data protection) took effect in EU law. Premised on the idea that, for change to be possible in law, the conditions ensuring that a certain degree of consistency is maintained must be in place, a sub-question that needs imperatively to be addressed is: How has EU law achieved sufficient consistency as to allow for this concrete change to take place? Or, in other terms: How did EU law, prior to the appearance of the fundamental right to the protection of personal data, accommodate its absence, while at the same time potentially permitting a consistent materialisation of its existence?

The phenomenon explored is described as the *emergence* of the EU right to personal data protection in the understanding that this term refers to the whole process of the right's coming into being, including the legal conditions surrounding this surfacing. What is explored is not only how did the right develop, but also how was it possible for this to happen, and how did it occur.

[10] In this sense, for instance: (Braibant 2001, p. 47; Loncle 2002, p. 45; Vitorino 2003, p. 117; Battista Petti 2006, p. 247; Ehlers 2007, p. 382; Pérez Luño 2010, p. 623; Bignami 2009, p. 139; Kühling 2011, p. 489). Portraying it as advancing a curious approach to personal data protection: (Büllesbach et al. 2010, p. 3).

[11] Using the image of a 'game of influences': (García-Berrio Hernández 2003, p. 15).

The research inquiries *how* could a specific legal change take place, rather than *why* this change occurred. This is so because it aims to explore the way in which law evolves, rather than to search for reasons attempting to explain such evolution from a non-legal perspective. This approach does not pretend to refute the existence of a context in which law operates, or its possible significance. On the contrary, it stresses that such context can affect and permeate law, even though only through legal occurrences; thus, by integrating law and becoming law.

1.3 Scope and Limitations

Tracing out law's functioning in search for answers to these questions, the book examines the EU's involvement in the area of personal data protection, and necessarily also the way in which EU law connections to other legal systems have determined (and continue to determine) this involvement.

The exploration helps to illuminate what could be the meaning of the EU right to the protection of personal data, and the possible significance of its status as EU fundamental right. The right being relatively novel, literature about it is still fairly limited. Major investigations concerned with European personal data protection have often privileged the overview of EU data protection instruments and principles (Bygrave 2002), or applicable law (Kuner 2003), as opposed to an in-depth study of the particular fabrication of the EU fundamental right.[12]

The research is undertaken without relying on any pre-conceived definition of the content of the EU right to the protection of personal data, or even of personal data protection as a legal notion in abstract.[13] It is therefore confronted with the challenge of investigating the way in which emerged a notion that it refuses to circumscribe in advance.

To address this conundrum, it is assumed that the origins of the EU right to the protection of personal data might be traced back to the earliest manifestations of (what came eventually to be known as) 'data protection' law in Europe. Concretely, the book identifies as the symbolic starting point of EU data protection the adoption of the first legal instrument bearing the name of *Datenschutz* (a German composite word, translatable as 'data protection'), namely, the Data Protection Act of the German federal state of Hesse of 1970. From there, it attempts to unearth the paths leading to the recognition of the right to personal data protection as enshrined by the EU Charter, studying the progressive acknowledgment of the notion as a fundamental right, but also the roots of the six basic components that constitute requirements applicable to any processing of personal data according to Article 8 of the EU Charter: (a) the principle of fair processing; (b) the principle of purpose specification; (c) the principle of need of a legitimate basis, which might be the consent of the person concerned; (d) the right of access; (e) the right to have data rectified; and (f) the principle of independent supervision.

[12] As notable exceptions: (Siemen 2006; Arenas Ramiro 2006; Coudray 2010).

[13] As a matter of fact, it is debatable whether any legal notions can be described in such manner.

In tracking down progress from the initial instances of data protection in Europe to the right to personal data protection as a EU fundamental right, the investigation soon encounters a legal notion of non-European origin: 'privacy' as referring to control over personal information, a concept that saw the light not in Europe, but in the United States (US), and actually sprang up before 1970s: by the end of the 1960s. The notion's significance in the process leading to the emergence of the EU right to the protection of personal data appears since the outset as being (at least) dual: first, its advent responded to concerns similar to those that prompted the surfacing of data protection laws in Europe; second, as a result of its usage in the US, the word 'privacy' was integrated as such into international and European legal instruments in the field of personal data protection and, partly as a result of this, eventually also entered EU law. Taking this into account, and despite its central focus on the right to the protection of personal data in EU law, the book also incorporates an exploration of the birth of the notion of privacy as control over personal information in the US.

The research does not terminate with the inclusion of the right to the protection of personal data in the 2000 Charter, but examines also the subsequent, post-2000 gradual assimilation of the right to the protection of personal data in EU law: concretely, in EU primary and secondary law, and in the case law of the EU Court of Justice. It additionally considers the legislative package introduced by the European Commission in January 2012 for the review of the EU personal data protection legal framework. In this package, the European Commission endorsed the existence of the EU right to personal data protection by placing it at the centre of future EU legal instruments in the field, heralding the almost complete disappearance from these instruments of the term privacy.

In sum, the book's material scope covers the advent of the right to the protection of personal data as a EU fundamental right starting from the earliest steps of data protection law in European countries up to the right's enshrinement in the EU Charter, and later incorporation in EU law, as well as its recognition by the EU Court of Justice. And it includes, as background, the prior development in the US of the notion of privacy as informational control, the prolonged embroilment of European (personal) data protection and privacy, and the announced vanishing of privacy from EU personal data protection law.

The research does not aim to provide an exhaustive historical account of personal data protection in Europe, or even in EU law. Similarly, it does not pretend to offer an overall analysis of the evolution of personal data protection (or privacy) in any specific Member State. It refers to such developments only insofar it is necessary and useful to illuminate the emergence of personal data protection as a EU fundamental right.

Because it focuses in studying law, the research might appear to set aside the relevance of factors other than law itself for explaining the change at stake. In relation to privacy and personal data protection, a factor customarily brought to the fore is technology. Technology is actually repeatedly mentioned both as a factor possibly justifying the birth of these legal notions, and their (regularly anticipated) demise.[14]

[14] Relativizing the importance of technology for the evolution of privacy as a legal notion: (Rigaux 1997, pp. 135–136).

Examples abound in the literature of attempts to apprehend, and communicate, how technology supposedly acts upon this legal field. They typically endeavour to pinpoint technological changes of a certain ubiquity,[15] nature or magnitude[16] that inescapably affect, or shall affect, law. Without dismissing the relevance of technology in this area, this research deliberately addresses it through the lens of law. Any technological consideration not incorporated by law is thus beyond the scope of this book.

The aim of this choice is not to negate the relevance of technology for the development of personal data protection, but to problematise it. The basic assumption behind this standpoint is that the exploration of what law does with technology, as well as of what technology does with law, can both have an explicative value for law's evolution, but that, whatever these events might be, they must take place (to be relevant for law) within law with the words of law: expressed in terms that evoke law's peculiar mode of existence, they must have entered the fabric of the legal.[17]

1.4 A Study of Change in (EU) Law

To investigate the emergence of the EU fundamental right to personal data protection, particular attention has been granted to language. This choice deserves some clarifications.

1.4.1 Multilingualism and EU Law

The foregrounding of language in the study of EU law is commonly identified with the coexistence of multiple languages in the EU, and with their peculiar treatment by EU law. These two features are often referred to as the 'multilingualism' of the EU, and of EU law.

[15] Devices are commonly portrayed as potentially having a major impact in the field when initially appearing in the market. See, for instance, on the transistor as a threat: Commission on Human Rights of the United Nations Economic and Social Council, Human rights and scientific and technological developments: Report of the Secretary-General (Addendum 1), E/CN.4/102, 26.2.1970; on the tape recorder as a threat: (Packard 1971, p. 16).

[16] Descriptions of unprecedented expansions of data processing capabilities are perhaps the most challenging for authors and readers alike (for instance, asserting that ten reels containing each 1.500 meters of tape 2,5 centimetres wide could store a 20-page dossier on every man, woman and child of the world: (Robertson 1973, p. viii); noting that a single optical disk can store four billion characters, comparable to 40 reels of tape: (Flaherty 1989, 2). Some authors chose to illustrate the significance of the issue at stake by providing figures on the number of users; for instance, noting the existence of an estimated 97 million Internet users in 1998: (Tan, p. 664).

[17] See notably, on this perspective: (Gutwirth 2010).

Multilingualism has marked EU law since its very origins.[18] Already in 1952, four languages of what were later to become the six founding Member States of the European Economic Community (EEC)[19] (that is, Belgium, France, Germany, Italy, Luxembourg, and the Netherlands) were put forward as its official and working languages: French, German, Dutch and Italian (Berteloot 2000, p. 347). Since the beginning, the EEC construed its multilingualism on the basis of the principle of equality between official languages (Rideau 2007, p. 63). This approach has survived through the decades, even if the number of official languages has significantly increased. As a result of the different accessions of new Member States, the EU incorporated as official languages English and Danish, in 1973; Greek, in 1981; Spanish and Portuguese, in 1986; Finnish and Swedish, in 1995; Czech, Estonian, Hungarian, Latvian, Lithuanian, Maltese, Polish, Slovak, Slovene, in 2004; Irish,[20] Bulgarian, and Romanian, in 2007; and Croatian, in 2013.

Multilingualism is nowadays regarded as consubstantial with EU law (Derlén 2009, p. 3). It is as such enshrined in the Treaties.[21] All versions of EU legal instruments in the 24 official languages are regarded as equally authentic, and in principle all legal acts of the EU shall be published in all official languages.[22]

EU multilingualism affects both law making and adjudication, but each EU institution can apply it differently. Although official languages are in theory also 'working languages' everywhere,[23] each institution might stipulate particular obligations in its own rules of procedure.[24] The European Parliament has traditionally put special emphasis on multilingualism across its activities. In the Council and the European Commission, the working languages are primarily English and French, and to some extent German (Derlén 2009, p. 5). Before the Court of Justice of the EU, any EU official language can be used,[25] but the judgments of the Court (unlike other EU documents) are only authentic in the language of the case.[26] The EU Court's working language has traditionally been French (Derlén 2009, p. 5).

EU law's own multilingualism evolves in the context of the system's pervading linkages with other legal systems and instruments. Thus, in addition to being multilingual per se, EU law is intrinsically connected to other systems that might also

[18] The key instrument in EU secondary law is: Regulation No 1 determining the languages to be used by the European Economic Community [1958] OJ L17/385.

[19] Which would eventually become the EU.

[20] Irish had acquired in 1973 'Treaty language' status.

[21] Consolidated version of the Treaty on European Union (TEU) [2010] OJ C83/13, Article 55.

[22] Two derogations from Article 4 of Regulation No.1, which provides for the simultaneous publication of the Official Journal of the European Union in all the official languages, have been foreseen: for Maltese in 2004 and for Irish in 2005.

[23] Article 1 of Regulation No 1.

[24] Ibid. Articles 6 and 7.

[25] Article 29 of the Rules of Procedure of the EU Court of Justice establishes that all EU official languages can be used before the Court; with some exceptions, the plaintiff has the right to choose the language of the case (Rules of Procedure of the Court of Justice of the European Union [1991] OJ L176/7 and further amendments).

[26] Ibid. Article 31.

have a (different) multilingual nature, and with which it will often share the use of sometimes one, but often more, natural languages. As a notable example, EU law grants a particular relevance to instruments emanating from the Council of Europe, such as the ECHR, and to the case law of the ECHR's maximum interpreter, the European Court of Human Rights (ECtHR). The Council of Europe is an international organisation that has 47 member countries, including all EU Member States, but a different linguistic regime, grounded on the (mere) coexistence of French and English.

EU law is also intertwined with the national legal systems of EU Member States. Contrary to international treaties, typically more self-contained, EU law directly enters into national law (Cielito Lindo Kommunikációs Szolgáltató Bt. 2010, p. 69). There exists therefore, inevitably, a continuous interaction between the national and EU usages of legal terms of a same natural language.[27] Moreover, some EU official languages (such as French, German, Dutch, English and Greek) simultaneously pertain to different national systems, and thus, in these systems, national provisions coexist with others emanating from the EU in a language which is not specific to them, but shared by various Member States.[28]

In this context, the question arises as to whether the usage of a particular language in EU law can be considered equivalent to the usage of the same language in interconnected (international and national) laws. EU law being an autonomous legal system, it produces and sustains its own legal terminology. The EU Court of Justice has in this sense emphasised that there are some terms that must imperatively be given an autonomous (EU) interpretation throughout Member States, different from the interpretation applicable to the same words in national law. The boundaries between sets of usages are however not always crystal-cut (Kjaer 2011, p. 332).[29]

The differences in meaning of words pertaining to a specific natural language when used in distinct legal contexts can be designated as 'intra-linguistic' issues. An illustration of the phenomenon could be the word 'privacy' in US law, compared with 'privacy' in the British legal system.[30] Any investigation of the functioning of EU law must in any case be aware of these possible intra-linguistic nuances, and discrepancies, which can imply that, for instance, the French expression *vie privée* as used in the ECHR might not be fully comparable to the same expression as operating in French or Belgian law, or that the German word *Datenschutz* might not have the same meaning as the same word in a German version of a EU legal instrument.

The multilingualism of EU law and of its related legal systems does not only generate intra-linguistic issues. Additionally, and perhaps even more frequently, it brings to the fore the question of translation.

---

[27] Ibid.

[28] Ibid. 70.

[29] On the alien character of the language of ECtHR judgments: (Kjaer 2011, p. 328).

[30] Summarising such difference as a contrasting envisioning of 'privacy' as tort: (Glanert 2009, p. 280, 2011, p. 187).

1.4.2 Translation and EU Law

The significance of translation for the purposes of EU law has attracted the attention of different disciplines,[31] which in their turn tend to rely on very diverse conceptions of translation.

EU's multilingualism inevitably entails a significant amount of concrete translation acts. The working languages of EU institutions involved in the legislative process being essentially French and English, many EU legal instruments in other officially 'authentic' languages de facto constitute translations from an original in French, or in English (Derlén 2009, p. 5). Translation is also part of judicial practice, be it at the EU Court of Justice, or as national courts and judges are confronted with the interpretation and application of EU law (Kjaer 2011, p. 328). EU legal instruments being always inscribed in a framework where are enacted simultaneously different languages and multiple language combinations, EU's multilingualism generates specific practical challenges for all actors—not only for legal translators, but for anyone concerned with the reading and writing of EU law.

Prototypically, a certain idea of translation might be described as the transfer of meaning from one language (the 'source language') into another (the 'target language') (Kjaer 2011, p. 328). From this perspective, phenomena such as mistranslations can be acknowledged: they would constitute transfers of meaning that can be regarded as inaccurate. In this sense, one of the major sources of difficulty when translating is the problem known as of 'non-equivalence', allegedly taking place when a legal term in one (source) language does not appear to correspond clearly to any existing term in another (target) language (Cao 2009, p. 21), rendering difficult the search for a word ensuring accurate transfer of meaning.

To avoid mistranslations despite the perceived lack of an equivalent word in the target language, a possible strategy is to incorporate a word from the source language directly into the target language, with the purpose of attributing to it exactly the same original meaning (or at least one of its meanings). This procedure, labelled as 'direct translation', can take different forms (Munday 2008, p. 56). One is 'borrowing', which occurs when a word is transferred as such into the target language; this is what has seemingly happened for instance in some European languages such as Dutch, or Italian, which have adopted the English word 'privacy'. Another common procedure is commonly referred to as 'calque', and amounts to mirroring the original structure in the most literal way possible (Munday 2008, p. 56); this is how the German *Datenschutz* was integrated into English as 'data protection'.

The notion of borrowing, in the sense of terminology imports from one language into another, has outstandingly been put to use in the area of comparative law. Rethought as 'legal borrowing',[32] it has been envisaged basically as the relocation of

[31] And inter-disciplines, such as translation studies; see, for instance: (Munday 2008)). The concept of translation has also been notably used in the context of Science, Technology and Society (STS) studies; see, for instance: (Akrich et al. 2006).

[32] A notion which has also lead to related ideas such as 'constitutional borrowing' (Robertson 2004, p. 54).

legal terms from one legal system to another, typically involving simultaneously an inter-lingual move. These relocations where initially commonly referred to as 'legal transplants' (Watson 1995),[33] and later increasingly as 'legal transfers' (Graziadei 2008, p. 443). This research area has illustrated that the transfer of a legal term into a new legal system triggers complex patterns of change (Graziadei 2008, p. 442), and, more generally, that the translation operations taking place whenever different legal systems interact can have important effects and consequences on the evolution of each system (Cao 2009, p. 4). A notion surfaced in this context is the idea of 'productive misreading(s)' (Mattei 2008, p. 827), which aims to emphasise that translation operations can sometimes be based on misinterpretations of a word's original meaning, but that they will, nevertheless, still generate meaning.[34]

Strictly speaking, however, there is in principle no such a thing in law as a mistranslation. If a EU legal instrument uses the word x in one of its language versions as synonym for the word y of another language version, for the purposes of EU law the two words shall have the same meaning, and this regardless of any linguistic consideration on the possible difference or even incompatibility of meanings between x and y.[35] This derives from the principle of equality of meaning of different language versions of the same text, one of the legal fictions sustaining the functioning of EU law.[36]

Hence, when a EU legal instrument uses the word x in one of its language versions as a synonym for the word y in another language version, EU law is configuring and endorsing them as synonym. Similarly, when a EU legal instrument asserts that an international instrument external to EU law enshrines a right under a certain label, it renames it for the purposes of EU law: for instance, when Directive 95/46/EC[37] declares that Article 8 of the ECHR recognises a right 'to privacy', it establishes that, for the purposes of the Directive, this is so even if Article 8 of the ECHR does not allude to any right 'to privacy', mentioning instead a right 'to respect for private life'.

[33] See also, on the notion of legal transplants and its reception: (Choudry 2006, p. 17).

[34] This idea is also at the core of the metaphor of 'legal irritants': (Teubner 1998, p. 12).

[35] If their equivalence in meaning is disputed, the judiciary might be required to intervene to explain how to reconcile in practice their apparent different meaning with the necessity of their equivalent interpretation (as far as the EU Court of Justice is concerned, reconciliation will be typically sought after through teleological interpretation; see, for instance: (Fennelly 1996). See also: C-29/69 Stauder v Stadt Ulm [1969] ECR 419, Judgment of the Court of 12 November 1969; C-30/77 Régina v Bouchereau [1977] ECR 1999, Judgment of the Court of 27 October 1977. If the interpretation of some linguistic versions of EU provisions is legally disputed on the grounds of the ambiguity of the provisions' wording, the EU Court of Justice can also decide to impose their reading in the light of what it identifies as 'unequivocal language versions' (see: C-90/83 Paterson v Weddel [1984] ECR 1567, Judgment of the Court (First Chamber) of 22 March 1984, concerning the meaning of 'animal carcasses').

[36] On the fictional nature of this assumption, see for instance: (Bellos 2011, pp. 237–241). Equivalent considerations are applicable to translations substantiated and endorsed by case law (Kjaer 2011, p. 331).

[37] Recital 10 of Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

1.4.3 Translation, Untranslatability and Law

The pervasiveness of translation in EU law appears to run counter to the conception that some words, and especially some legal words, are particularly difficult or even impossible to translate. The truth is that any perception of a peculiar untranslatability of some legal terms is regularly put into question by the profusion of translation operations involving these terms, taking place not only in EU law, but more broadly in international law. In this sense, 'privacy' has sometimes been singled out as an untranslatable term (Anderman and Rogers 2003, p. 33, 73), but, actually, it is mentioned in the Universal Declaration of Human Rights, proclaimed by the General Assembly of the United Nations (UN) in 1948,[38] which has been identified by the Guinness Book of Records as the most translated document in the world. The allegedly untranslatable word has been repeatedly translated.

The notion of untranslatability can actually also be understood differently: not as a (possible) characteristic of some specific terms, but as a condition inherent to all words. The fundamental condition of words as untranslatable is the conceptual corollary of a certain understanding of how meaning is set through words, or, rather, never set, but permanently sustained as unsettled.[39] This conception of the relation between words and meaning places at the core of meaning's generation the fact that meaning is in words forever unresolved (Derrida 1967, p. 102), and will only be resolved through reading. Words are perceived as characterised by estrangement. They are never fully present but marked, instead, by traces (Derrida 1967, p. 102) of (apparently) absent meaning that only reading and re-writing can reinstate. If meaning is ungraspable, a certain type of translation (envisaged as the replication of meaning from a language into another) becomes impossible (Legrand 2011, p. 616). Untranslatability arises thus as a resistance to adscription to meaning (Derrida 2008, p. 233), inherent to all words.

This concept of untranslatability has a number of consequences for the study of law. Notably, it invites to downplay the distinction between some words supposedly difficult to translate and the rest, emphasising that, ultimately, it is impossible to fully and completely accurately translate any word. This idea of untranslatability also hints at the relevance for the determination of words' meaning of the practice of reading and re-writing, which might even involve reading and re-writing in other languages: words might bear (invisible) traces and connections with other languages, and thus be regarded as quintessentially hybrid, polyglot (Derrida 1998, p. 33), multilingual.[40] From this standpoint, it becomes advisable not to envisage relations between legal systems as interactions between separate languages representing dis-

[38] Article 12 of the Universal Declaration of Human Rights establishes that '(n)o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation'.

[39] The unsettlement of meaning in words has notably been portrayed by French philosopher Jacques Derrida, who addressed the matter through the notion of différance (Derrida 1967).

[40] In reality, Derrida asserts the multilingualism of all words (Derrida 1996, p. 21). On the ubiquity of Babel, see: (Ost 2009, p. 24).

tinct and separate models or traditions (Derrida 1998, p. 35), but to recognise that models, traditions, and languages are profoundly interwoven. Acknowledging that words are marked internally by breaks and traces that can disrupt meaning is, in its turn, an invitation to investigate words historically,[41] and to analyse how have been articulated, through time, the entanglements between a word and the possible meanings it sustains as unresolved (Derrida 1967, p. 229).

Furthermore, embracing this foundational untranslatability of words can lead to a renewed appreciation of translation.[42] The reconstructed notion would not focus on the fact that translating a word is an attempt to reproduce a certain meaning imported from an original source into a target language, but rather revolve around the inevitable failure that this venture will encounter, and on the resulting instabilities and displacements of meaning(s) to occur (Legrand 2003, p. 291). All translations are, in this sense, mistranslations, and will result in a *décalage*, a shift, a (productive) gap (Legrand 2009). Translation is envisaged thus not as primarily playing a replicating role, but as having a re-creating function. It is an exercise of reading and re-writing, and thus of settlement and re-setting in motion of meaning. Thus, untranslatability and the pervasiveness of translation are therefore assumptions that can coexist.[43] The former underlines the struggle of trying to ascribe meaning to words, and the latter highlights how such struggle is ubiquitous and will, in any case, always allocate meaning.

The perception of meaning as always to come can be also applied to the functioning of law. In this sense, law is also always to come, always deferred, and will only take place as a singular differentiation (Derrida 1993, p. 37) that, once occurred, leaves law again open to multiple and unsettled differentiations. It is not merely words in general, but also the very words of law, that are permanently subject to review in the light of distinctions to come (Luhmann 2009, p. 242). In association to the untranslatability of words, springs up the notion of law's undecidability.

1.4.4 Undecidability and Change in Law

Law's undecidability refers to the tension between the idea that law must always be determined, resolved, settled (in this sense, it is imperative for courts to decide on the meaning of law) and the fact that, for law to be meaningfully decided, it has to be previously (profoundly, genuinely) undecided (Derrida 2005, p. 53). Paradoxically, courts must always decide, but can only decide because the undecidability of law is given as a matter of principle (Luhmann 2009, p. 282). And, despite systemically deciding on the meaning of law, courts never resolve its undecided nature. Just as meaning is permanently unresolved in words, only punctually settled in reading

[41] For instance, apprehending them as a hauntology (Legrand 2006, p. 524). See also: (Legrand 2008, p. 373). On hauntology, see: (Derrida 1993, p. 31).

[42] In this sense: (Davis 2011, p. 74).

[43] Also in this sense: (Derrida 2008, p. 238).

and invariably re-destabilised through writing, configuring a continuous process of meaning condensation and amplification (Luhmann 2009, p. 240), meaning in law is transformed as a consequence of the multiple singular occurrences of law (through continually renewed distinctions and in-distinctions), but never fixed.

The notion of law's undecidability has fruitful repercussions in the understanding of how law evolves. It was notably employed by German sociologist Niklas Luhmann,[44] who emphasised law's work as a text in the sense that, through its operations, law constantly (re)organises references to meaning (Luhmann 2009, p. 242).[45] Luhmann's conception of law as text should not be interpreted as restricting law to written legislation, as it definitely includes decision-making by courts, which are in point of fact regarded as the paradigmatic location in which the problem of unfolding the undecibidability of law has to be solved (Luhmann 2009, p. 291).[46] Law as text also integrates, nevertheless, a variety of other premises that can take effect as law (Pottage 2012, p. 176).

This conception of law as text stresses that the connections between occurrences of law do not lead only to repetition and reinstatement, but also to recreation (García Amado 1989, p. 27). From this perspective, legal evolution surfaces as an outcome of the reading and re-writing of law by law. This reading and re-writing always involves a degree of interpretation (Luhmann 2009, p. 243), and thus of contingency, but requires simultaneously requires a degree of consistency that will guarantee the connection among the multiplicity of decisions (Luhmann 2009, p. 318). The needed consistency can be described as 'redundancy', or the faculty of a legal occurrence to reduce its element of surprise (Luhmann 1994, p. 61).[47] The tensions between variation and uniformity are played out through the unresolved status of meaning in words.

Hence, to study how law changes, as well as changes in law, it is necessary to track down traces waiting for unfolding, and to engage in a recollection of what has come to constitute (the text of) law (Legrand 2011, p. 609). A complete unearthing of relevant traces might be unachievable (Legrand 2011, p. 613), but the exercise can possibly be regarded as accomplished if it helps to explain a particular movement—in this case, the emergence of the protection of personal data as EU fundamental right.

---

[44] On the relation between Derrida and Luhmann, See: (Teubner 2001, p. 30). On the importance of distinction for Niklas Luhmann, see: (Guibentif 2010, p. 124).

[45] Luhmann envisages law as made of communications referring recursively to other communications, ensuring through such referencing their connectivity as elements of the system, and constructing through at the same time their meaning (something which, in his own terminology, constitutes a 'social system') (Luhmann 2009, p. 98). His conception has been criticised by some theorists, notably French sociologist and anthropologist Bruno Latour (Latour 2004). Despite this explicit rejection, others have emphasised that many of Latour's insights about law are actually fully consistent with Luhmann's theory (Pottage 2012, p. 175).

[46] This idea can be interpreted as echoing the identification of case law as the place where law is created (Deleuze 2003, p. 209).

[47] Describing judges as the masters of the art of camouflage of the innovative dimensions of their constructions: (Ost 1998, p. 94). On the opportunistically alleged links with the ancient of US privacy constructs, for instance: (Posner 2001, p. 153).

1.5 Outline

The book is structured in two parts. Part I is composed of Chaps. 2, 3 and 4, and is primarily concerned with developments external to the EU that historically influenced the appearance of personal data protection provisions in EU law. Many of these developments are also directly relevant for the interpretation of existing EU data protection law, and of the EU fundamental right to the protection of personal data, through their various connections to the EU legal system.

Chapter 2's main objective is to explore the usages of the term 'privacy' prior to (and contemporary with) the advent of 'data protection' laws in Europe. After an introductory overview of the multiplicity of meanings commonly ascribed to privacy, it focuses on examining the redefinition of the notion as it unfolded in the US at the end of the 1960s, and on how this redesign attempted to make 'privacy' immediately relevant for the protection of individuals against the automated processing of information about them. Having described the historical linkage between the issue of computers and (a redefined) privacy, as well as the inscription of privacy in US law, the chapter accounts for a number of efforts that surfaced internationally, and particularly in Europe, to address through a 'privacy' lens (some of the) challenges posed by technological developments—be it by using or looking for the very word privacy, or words envisioned as synonymous in other languages.

Chapter 3 is devoted to the surfacing in European countries of provisions aimed at regulating the processing of data about individuals since the beginning of the 1970s, and up to the end of that decade. It contains two main sections: one on the first European legal instruments that specifically targeted the processing of data about individuals, and another on countries where, since the very first moment, the choice was made to circumscribe the limits of (automated) personal data processing through constitutional provisions. As prime examples of the first category are described the cases of the federal state of Hesse, Germany, Sweden and France. And, as instances of the second approach, constitutional recognition in Austria, Portugal and Spain is studied and discussed.

Chapter 4 centres on pioneering international 'data protection' instruments. Its major objective is to analyse the design of Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), which had a major influence on the drafting of EU legislation, as well as on national legal systems, with the view to understand better how it affected the legal construction of the words 'privacy' and 'data protection' in Europe. The elaboration of Convention 108 ran in parallel with work on the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD), adopted in 1980, which is also examined. The chapter also inquiries into the initial impact of Convention 108 on the development of national instruments in European countries, as well as on the evolution of ECtHR case law on the right to respect for private life as enshrined by Article 8 of the ECHR.

Part II focuses more concretely on EU law. It also comprises three chapters. The first, Chap. 5, considers EU involvement in the regulation of personal data

processing, from its initial steps until the year 2000. First, it examines early inter-institutional discussions on the subject. Second, it scans the development of EU law, granting particular attention to Directive 95/46/EC, but considering also Directive 97/66/EC and other developments both in primary and secondary EU law. The chapter additionally explores the impact of these developments on national laws regulating the processing of personal data.

Chapter 6 investigates the inscription of personal data protection among EU fundamental rights. It studies the changing EU approach to fundamental rights, including historical turns in case law, and early attempts to write down a EU-specific fundamental rights catalogue. To determine the plausibility of considering the protection of personal data as a common constitutional tradition of EU Member States, it reviews the framing in national legal systems of the fundamental rights' dimension of data protection laws. The chapter concludes with an account of the drafting of the EU Charter, and an analysis of its relation with the protection of personal data, both through Article 7 and Article 8 of the 2000 instrument.

Chapter 7 is dedicated to the materialisation of the EU right to the protection of personal data in EU law following the proclamation of the EU Charter. It has two main sections: one examining the status of the right before the entry into force of the Treaty of Lisbon in 2009, and another on the evolution afterwards. The first examines the integration of the right to the protection of personal data in EU secondary law, and in the case law of the EU Court of Justice, until 2009. The second addresses the main relevant changes brought about the Lisbon Treaty, explores the post-Lisbon case law of the EU Court of Justice, and scrutinises the legislative package presented by the European Commission in January 2012 for the future of EU personal data protection.

Chapter 8, on the basis of the findings of the previous chapters, puts forward concluding remarks, and discusses them in the wider perspective of existing knowledge in the area.

1.6 Sources

This study is based on information from publicly accessible sources including international, national and EU legislation and relevant case law, as well as legal and non-legal publications. The law is dated as at September 2013.

References

Akrich, Madeleine, Michel Callon, and Bruno Latour. 2006. *Sociologie de la traduction*: *Textes fondateurs*. Paris: Écoles des mines de Paris.

Anderman, Gunilla M., and Margaret Rogers, eds. 2003. *Translation Today: Trends and Perspectives*. Clevedon: Multilingual Matters.

Arenas Ramiro, Mónica. 2006. *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant Lo Blanch.
Battista Petti, Giovanni. 2006. *La Costituzione Europea e la tutela civile dei Diritti Umani (Aggiornato alla legge 15 dicembre 2005, N. 280)*. Santarcangelo di Romagna: Maggioli Editore.
Bellos, David. 2011. *Is That a Fish in Your Ear? The Amazing Adventure of Translation*. London: Penguin Books.
Bernsdorff, Norbert. 2003. Kapitel II, Freiheiten: Artikel 6 Bis 19. In *Kommentar zur Charta der Grundrechte der Europäischen Union,* ed. Jürgen Meyer, 135–262. Baden-Baden: Nomos Verlagsgesellschaft.
Berteloot, Pascale. 2000. Le droit à la langue de l'Union européenne. In *Langue et Droit,* ed. Erik Jayme, 345–362. Bruxelles: Bruylant.
Bignami, Francesca. 2009. Constitutional patriotism and the right to privacy: A comparison of the European Court of Justice and the European Court of Human Rights. In *New Technologies and Human Rights,* ed. Thérèse Murphy, 128–160. Oxford: Oxford University Press.
Braibant, Guy. 2001. *La Charte des droits fondamentaux de l'Union européenne*. Paris: Editions du Seuil.
Brosig, Malte. 2006. Human rights in Europe: An introduction. In *Human Rights in Europe: A Fragmented Regime?* ed. Malte Brosig, 9–29. Frankfurt a. M.: Peter Lang.
Büllesbach, Alfred, Serge Gijrath, Yves Poullet, and Corien Prins, eds. 2010. *Concise European IT Law*. 2nd ed. Alphen aan den Rijn: Kluwer Law International.
Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.
Cao, Deborah. 2009. *Translating Law*. Clevedon: Multilingual Matters.
Choudry, Sujit. 2006. Migration as a new metaphor in comparative constitutional law. In *The Migration of Constitutional Ideas,* ed. Sujit Choudry, 1–35. Cambridge: Cambridge University Press.
Cielito Lindo Kommunikációs Szolgáltató Bt. 2010. *Study on lawmaking in the EU multilingual environment*. Studies on Translation and Multilingualism. European Commission, Directorate General for Translation.
Coudray, Ludovic. 2010. *La protection des données personnelles dans l'Union européenne*: *Naissance et consécration d'un droit fondamental*. Berlin: Éditions universitaires européennes.
Davis, Kathleen. 2011. Deconstruction. In *Routledge Encyclopedia of Translation Studies.* 2nd ed. eds. Mona Baker and Gabriela Saldanha. London: Routledge.
Deleuze, Gilles. 2003. *Pourparlers (1972–1990)*. Paris: Les Éditions de Minuit.
Derlén, Mattias. 2009. *Multilingual Interpretation of European Union law*. Alphen aan den Rijn: Wolters Kluwer.
Derrida, Jacques. 1967. *De la grammatologie*. Paris: Les Éditions de Minuit.
Derrida, Jacques. 1993. *Spectres de Marx*. Paris: Éditions Galilée.
Derrida, Jacques. 1996. *Le monolinguisme de l'autre ou la prothèse d'origine*. Paris: Éditions Galilée.
Derrida, Jacques. 1998. *Le droit à la philosophie du point de vue cosmopolitique*. Lagrasse: Éditions Verdier.
Derrida, Jacques. 2005. *Force de loi*: *le "fondement mystique de l'autorité"*. Paris: Éditions Galilée.
Derrida, Jacques. 2008. *La Bête et le Souverain Volume I (2001–2002)*. Paris: Éditions Galilée.
Ehlers, Dirk. 2007. The fundamental rights of the European Union: General principles. In *European Fundamental Rights and Freedoms: General Principles*, ed. Dirk Ehlers, 371–398. Berlin: De Gruyter.
Fennelly, Nial. 1996. Legal interpretation at the European Court of Justice. *Fordham International Law Journal* 20 (3): 656–679.
Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press.

García Amado, Juan Antonio. 1989. Introduction à l'oeuvre de Niklas Luhmann. *Droit et Société* 11/12:15–52.

García-Berrio Hernández, Teresa. 2003. *Informática y libertades: La protección de datos personales y su regulación en Francia y España*. Murcia: Universidad de Murcia.

Glanert, Simone. 2009. Comparaison et traduction des droits: À l'impossible tous sont tenus. In *Comparer les droits, résolument,* ed. Pierre Legrand, 280–311. Paris: Presses Universitaires de France.

Glanert, Simone. 2011. *De la traductibilité du droit*. Paris: Dalloz.

Graziadei, Michele. 2008. Comparative law as the study of transplants and receptions. In *The Oxford Handbook of Comparative Law,* ed. Mathias Reimann and Reinhard Zimmermann, 441–475. Oxford: Oxford University Press.

Guibentif, Pierre. 2010. *Foucault, Luhmann, Habermas, Bourdieu: Une génération repense le droit*. Paris: Lextenso.

Gutwirth, Serge. 2010. Composer avec du droit, des sciences et le mode technique: Une exploration. In *Les technologies de l'information au service des droits: Opportunités, défis, limites,* ed. Daniel Le Métayer, 24–42. Bruxelles: Bruylant.

Juarroz, Roberto. 2012. *Poesía vertical*. Madrid: Cátedra.

Kjaer, Anne Lise. 2011. European legal concepts in Scandinavian Law and language. *Nordic Journal of International Law* 80:321–349.

Kühling, Jürgen. 2011. Multilevel constitutional jurisdiction. In *Principles of European Constitutional Law (Revised second edition),* eds. Armin Von Bogdandy and Jürgen Bast, 479–514. Oxford: Hart Publishing.

Kuner, Christopher. 2003. *European Data Privacy Law and Online Business.* Oxford: Oxford University Press.

Latour, Bruno. 2004. *La fabrique du droit: Une ethnographie du Conseil d'Etat*. Paris: La Découverte/Poche.

Legrand, Pierre. 2003. The same and the different. In *Comparative Legal Studies: Traditions and Transitions*, eds. Pierre Legrand and Roderick Munday. Cambridge: Cambridge University Press.

Legrand, Pierre. 2006. On the singularity of law. *Harvard International Law Journal* 47 (2): 517–530.

Legrand, Pierre. 2008. *Comparative legal studies and the matter of authenticity*. Legal Studies Research Paper Series Research Paper No. 08-071. University of San Diego, School of Law.

Legrand, Pierre. 2009. *Le droit comparé: « Que sais-je ? » N° 3478*. Paris: Presses Universitaires de France.

Legrand, Pierre. 2011. Siting foreign law: How Derrida can help. *Duke Journal of Comparative & International Law* 21:595–629.

Loncle, François. 2002. La Charte des droits fondamentaux: Le référentiel des valeurs de l'Europe. In *La Charte des droits fondamentaux et le développement constitutionnel de l'Union européenne*, ed. Wolfgang Heusel, 43–50. Köln: Bundesanzeiger.

Luhmann, Niklas. 1994. Le droit comme système social. *Droit et Société* 11/12:53–67.

Luhmann, Niklas. 2009. *Law as a Social System*. Oxford: Oxford University Press.

Mattei, Ugo. 2008. Comparative law and critical legal studies. in Matias Reimann and Reinhard Zimmermann" In *The Oxford handbook of comparative law,* eds. Mathias Reimann and Reinhard Zimmermann, 816–836. Oxford: Oxford University Press.

Munday, Jeremy. 2008. *Introducing translation studies: Theories and applications (originally published in 2001)*. London: Routledge.

Murillo de la Cueva Pablo Lucas. 2009. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. In *El derecho a la autodeterminación informativa,* eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 11–80. Madrid: Fundación Coloquio Jurídico Europeo.

Ost, François. 1998. L'heure du jugement. Sur la rétroactivité des décisions de justice. Vers un droit transitoire de la modification des règles jurisprudentielles. In *Temps et droit. Le droit a-t-il*

pour vocation de durer? Time and Law. Is it the Nature of Law to Last? eds. François Ost and Mark Van Hoecke, 91–134. Bruxelles: Bruylant.
Ost, François. 2009. *Traduire: Défense et illustration du multinguisme*. Paris: Fayard.
Packard, Vance. 1971. *The Naked Society (originally published in 1964)*. Harmondsworth: Penguin Books.
Pérez Luño, Antonio Enrique. 2010. *Derechos Humanos, Estado de Derecho y Constitución.* 10th ed. Madrid: Tecnos.
Piñar Mañas, José Luis. 2009. Protección de datos: Origen, situación actual y retos de futuro. In *El derecho a la autodeterminación informativa*, eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 81–179. Madrid: Fundación Coloquio Jurídico Europeo.
Posner, Richard A. 2001. *Frontiers of legal theory*. Cambridge. Mass: Harvard University Press.
Pottage, Alain. 2012. The materiality of what? *Journal of Law and Society* 39 (1): 167–183.
Rideau, Joël. 2007. L'Union européenne face aux défis linguistiques. In *Interpréter et traduire*: *Actes du Colloque international des 25 et 26 novembre 2005, Faculté de Droit de Toulon,* ed. Jean-Jacques Sueur, 63–150. Bruxelles: Bruylant.
Rigaux, François. 1997. *La Loi des Juges*. Paris: Éditions Odile Jacob.
Robertson, Arthur Henry. 1973. Preface. In *Privacy and Human Rights: Papers by experts on an issue of growing importance given under the auspices of the European Convention on Human Rights*, ed. Arthur Henry Robertson, vii-x, Manchester: Manchester University Press.
Robertson, David. 2004. *A Dictionary of Human Rights*. 2nd ed. London: Europa Publications.
Siemen, Birte. 2006. *Datenschutz als Europäisches Grundrecht*. Berlin: Duncker & Humblot.
Tan, Domingo R. 1999. Personal privacy in the information age: Comparison of internet data protection regulations in the United Stats and European Union. *Loyola of Los Angeles International and Comparative Law Review* 21:661–684.
Teubner, Gunther. 1998. Legal irritants: Good faith in British Law or how unifying law ends up in new divergences. *The Modern Law Review* 61 (1): 11–32.
Teubner, Gunther. 2001. Economics of gift—Positivity of justice: The mutual paranoia of Jacques Derrida and Niklas Luhmann. *Theory, Culture and Society* 18:29–47.
Tzanou, Maria. 2013. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law* 3 (2): 88–99.
Vitorino, Antonio. 2003. La Cour de Justice et les droits fondamentaux depuis la proclamation de la Charte. In *Une communauté de Droit: Festchrift für Gil Carlos Rodríguez Iglesias*, eds. Ninon Colneric, David Edward, Jean-Pierre Puissochet, and Dámaso Ruiz-Jarabo Colomer, 111–126. Berlin: Berliner Wissenschafts-Verlag.
Watson, Alan. 1995. From legal transplants to legal formants. *The American Journal of Comparative Law* 43 (3): 469–476.

Part I
Before the European Union

Chapter 2
Privacy and the Protection of Personal Data *Avant la Lettre*

> *Ah, whoever it was who invented the idea of privacy, of a privacy, of a private home—was the greatest genius of all time.*
>
> (Mekas 2010)

Rules on the processing of information about individuals originally surfaced in European countries under various labels: in 1970, the German federal state of Hesse adopted a seminal act concerned with the establishment of *Datenschutz* (translatable as 'data protection');[1] in 1973, Sweden approved an act named *Datalag* (or 'Data Act');[2] in 1978, France endorsed a law entitled *informatique et libertés* ('computers and freedoms').[3] The terminological creativity of data processing regulation breaking out in Europe during the 1970s was accompanied by a relative fuzziness in relation with the purpose, or purposes, targeted by these new provisions (Bygrave 2002, p. 8).

Eventually, however, all these norms and similar rules later emerging in Europe were to be formally designated as constituting 'data protection' laws, and officially ascribed to the objective of serving, primarily, something called 'privacy'.[4] This chapter focuses on this word: privacy. It investigates its origins and significance, and its historical connections with the development of European rules on the processing of personal data.

2.1 Introducing Privacy

As a concept, privacy has been described as being 'in disarray' (Solove 2008), or prone to definitional instability (Bygrave 2010, p. 169). Scholars have elaborated many different theories about it, attesting of the multiple clusters of meaning surrounding the word.

[1] See Chap. 3, Sect. 3.1.1, of this book.

[2] Ibid. Sect. 3.1.2.

[3] Ibid. Sect. 3.1.4.

[4] See, for instance: (Bennett 1992, p. 13; Bennett and Raab 2006, p. 19).

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_2,

2.1.1 Mapping Privacies

An overview of the literature on privacy reveals the possibility to map out many of the most common acceptations of the term by dividing them into a few basic categories, corresponding to different meanings of the adjective 'private',[5] from which the English noun 'privacy' derives.[6] Schematically:

a. privacy can be understood as protecting what is envisaged as private as opposed to public,[7] be it:
   1. conceiving of public as referring to governmental authority (the State), or the community or society in general (Duby 1999, p. 18); private is thus read as 'not official', or 'not pertaining to the *res publica*', for instance because specifically related to family life, or to the home;[8]
   2. envisioning public as what is shared, exposed, common, open to the other; private is thus read as belonging to a closed space or realm,[9] unexposed, hidden, confidential, concealed, secret (Duby 1999, p. 18), let alone, devoted to introspection,[10] generally inaccessible, or out of reach;[11] but
b. privacy can also be understood as touching upon what is private in the sense of individual, personal, or one's own: from this viewpoint, to claim respect for somebody's 'private life' is to affirm their right to live as they choose, as opposed to controlled, alienated, or estranged (from society and from themselves).

This classification aims to illustrate that the meanings of privacy and private are sometimes construed in opposition to what is public, but not always. As a matter of fact, privacy as a legal notion—and particularly as a legal notion worthy of reinforced protection in certain legal systems—has often been pictured as associated with what is 'private' in the sense of individual, personal, one's own (group B).

---

[5] The adjective 'private' derives from the Latin *privatus*. In Latin, *privatus* was typically used in contrast to *publicus* and *communis*, and meant 'private, individual, own' (*Dictionnaire Gaffiot Latin-Français* 1934, p. 1239), as well as 'simple citizen' (ibid.) and 'withdrawn from public life' (Schoeman 2008, p. 116).

[6] The English word 'privacy' was rarely used as such before the sixteenth century (Onions 1966, p. 711).

[7] The adjective 'private' surfaced in English in the fourteenth century, precisely meaning 'not open to the public', and in the fifteenth century with the sense of 'not holding a public position' (ibid.).

[8] The Latin *privatus* represented a particular usage of the past participle of the verb *privare*, originally meaning 'bereave, deprive', and from which stemmed for instance the French *priver*, defined in nineteenth century French dictionaries as referring to taking something away from the wild nature and taking it to the familiar space of the home (Duby 1999, p. 17). The Latin noun *privatum* referred to private assets, including the home, and the idiom *in privato* meant 'inside the house' (ibid. 18).

[9] Sometimes metaphorically. See, for instance: (Serfaty-Garzon 2003).

[10] Alluding to a *ius solitudinis*: (Pérez Luño 2010, p. 339).

[11] According to Gavison, '(i)n its most suggestive sense, privacy is a limitation of other's access to an individual' (Gavison 1980, p. 428).

From this perspective, privacy has notably been connected with freedom: some have described it as the fortress of personal freedom (Sofsky 2009, p. 53), what ensures a freedom to establish individual paths in life, and the potential to resist interferences with this freedom (Gutwirth 2002, p. 2), as individual freedom par excellence (Rigaux 1992, p. 9), or as the protection of freedom itself (Bendich 1996, p. 441). Privacy has also been attached to the notion of individuality, as such the outcome of a historical construction of the person (Lefebvre-Teillard 2003, p. 1151) originated in the early Christianity (Bennett et al. 2001, p. 280), developed through the Middle Ages, and consolidated with the Enlightenment and the advent of modern constitutionalism.[12] Privacy in this light would not just be about any boundaries separating what pertains to the State from the private lives of people, but rather a barrier sheltering individuals against the arbitrariness of State power. Through the idea of individuality, privacy would also be directly linked to autonomy (Bygrave 2002, p. 133).[13]

Privacy in the sense of serving the realisation of individuals' own lives has furthermore been coupled with the notion of human dignity. This view's basic assumption is that it is inherent to human condition to develop freely, and that, therefore, human dignity must presuppose the acknowledgement of a degree of self-determination (Pérez Luño 2010, p. 324). Here, individuality is identified with the full development of personality (Edelman 1999, p. 509), a concept associated with the notion of personhood, or the quality of being a human being. Privacy, full development of the personality and personhood are sometimes also connected to (and through) the concept of identity,[14] a multifaceted notion[15] with several potentially relevant meanings: in particular, identity can be envisioned as personality, or individuality,[16] but also as what allows for identification (or individualisation) (Bioy 2006, p. 74), in the sense of being the sum of personal identifiers.[17] Identity, however, is also sometimes addressed as a key to refine the relation between privacy and freedom (Hildebrandt 2006).

In comparative constitutional law, the recognition of a right to privacy as a unitary right is a late phenomenon (Ruiz Miguel 1992, p. 76). It was preceded by the enshrinement of other notions such as the inviolability[18] of the home, or

[12] In Anglo-Saxon thinking, a major reference in this context is the notion of liberty as individual autonomy developed by John Stuart Mill, in his work *On Liberty* (Stuart Mill 1948). See also: (Ruiz Miguel 1992, p. 7; Pérez Luño 2010, p. 329).

[13] Autonomy is sometimes envisioned as closely related to freedom and self-determination (De Hert and Gutwirth 2003, p. 95).

[14] See, for instance: (Rodotà 2009, p. 22; Kahn 2003).

[15] As attempts to circumscribe it can be mentioned the concepts of identity-in-transformation (Luhmann 1998, p. 37), or the 'ipse' and 'idem' dimensions discussed by French philosopher Paul Ricoeur, highlighting that identity is dependent both the perception of the self as unique, and the continuity of space and time, or what is shared with others (Ricoeur 1990).

[16] See, notably: (Pino 2006).

[17] These two basic facets of identity can be traced back to the writings of John Locke (Locke 1998, pp. 200–202 especially).

[18] Historically sometimes referred to as 'sanctity' of the home. On the origins of legal 'sanctity' as inviolability (and its relation with 'sanction'), see: (Thomas 2011, pp. 62–63).

confidentiality of correspondence, legal notions in some cases later regarded subsumed into a general right to privacy, understood then as an umbrella right.[19]

The conceptual ramifications of different understandings of privacy sometimes overlap. It can be argued, for instance, that for individuals to be effectively able to live freely, they need to be assured that some facets of their lives are to remain undisclosed. In point of fact, features such as the inviolability of the home, or confidentiality of communications (which might appear as prime examples of the significance of the private/public distinction as per group A), have in reality surfaced historically associated with personal freedom (as in group B) (Martínez Martínez 2004, p. 62).[20] Respect of privacy as the individual's own life is also often depicted as requiring that persons are ensured a place, or a time, to be on their own ('in private') in order to allow for personal reflection and for the development of personal attitudes.[21] To be free, individuals would need that some facets of their lives are kept private, out of reach.

Conversely, the conceptual ramifications of different views on privacy can also occasionally conflict. There are conceptions of privacy that warn against granting an excessive emphasis to concrete understandings of what is private as opposed to what is public; some scholars have indeed advanced the idea that for persons to be effectively (free) individuals, they cannot be detached from what is social, and public.[22] To enjoy a private life in the sense of a life of their own, individuals would need more than a 'merely private' life: privacy shall consequently include the dimension of the individual directed towards the exteriority, or towards the other (Ruiz Miguel 1992, p. 5). To be free, individuals must not to be kept apart.[23]

Different conceptions of privacy and related legal notions rely sometimes on coincidental terminology, generating some ambiguities. The term 'sphere' is a prime example of this. Political scholars have often used the image of concentric spheres to describe different degrees of individuals' connexion to the polity: they have depicted the existence of an intimate sphere, a private sphere, a social sphere, or a

[19] Describing privacy as an umbrella term: (Solove 2006, p. 486).

[20] See also: (Hansson 2008, p. 110).

[21] For US sociologist Charles Wright Mills, for instance, privacy 'in its full human meaning' referred to the possibility of individuals to transcend their milieu by articulating their own private tensions and anxieties, and, to the extent that mass media in general, and television in particular, encroached upon such private articulation of resentments and hopes, they were to be regarded as a 'malign force' causing privacy's destruction (Wright Mills 2000, p. 314).

[22] German sociologist Norbert Elias, for example, emphasised that what transforms children into specific, distinct individuals are their relations with others, and that the different structures of interiority shaping individual consciousness are precisely determined by the outside world (Elias 1991, p. 58 and 65). The exclusionary effects of the private/public distinction have notably been discussed in relation to the detrimental consequences for women (Bennett and Raab 2006, p. 21). From this perspective, the qualification of what is private emerges as not neutral, but imposing that some issues must be kept hidden, and tends to exclude women from the public life of decision-making or social interactions. See, notably: (Scott and Keates 2005; Halimi 1992, p. xiii and xiv).

[23] Or de-prived of 'public life'.

public sphere.[24] The image of the sphere, however, has also been used to convey the idea of something that is not primarily about enclosing, demarcating or obscuring, but rather about allowing for operations by the outside to take place (Sloterdijk 2007, p. 28),[25] contributing in that way to subjectivity.

The usages of words related to 'spheres' are as a matter of fact numerous.[26] In German constitutional case law, an influential legal theory has emerged since the late 1950s. It is known as the 'theory of the spheres'.[27] On the basis of this theory, the German Federal Constitutional Court envisaged a series of concentric circles, or spheres, delineating different areas based on distinct degrees of the private (Alexy 2010, p. 236): the *Individualsphäre*,[28] the *Privatsphäre*,[29] and the *Intimsphäre*.[30] The term *Intimsphäre* builds upon the German word derived from the Latin *intimus* (Coronel Carcelén 2002, p. 19), which also resulted in the English word 'intimacy' (nowadays rarely used in legal writing),[31] and evolved in other languages to form words more often used as synonymous with privacy, such as the French *intimité* (Bureau de la Terminologie du Conseil de l'Europe 1995, p. 321), or the Spanish *intimidad* (Coronel Carcelén 2002, p. 19).

The German Federal Constitutional Court abandoned the theory of the spheres in 1983, but the doctrine has nonetheless deeply marked both German and non-German literature.[32] In Germany, the doctrine sometimes refers to the right enshrined by Article 8 of the ECHR as *das Recht auf die Privatsphäre* (or 'the right to private sphere') (Frowein 1985, p. 195),[33] even if it can also be called the *Anspruch auf Achtung seines Privatlebens*, or 'right to respect for private life' (Frowein 1985, p. 194). Some other European legal orders have integrated legal notions based on cognates of the word sphere. The Dutch Constitution, for instance, grants individu-

[24] See, notably: (Arendt 1998, p. 38). For Arendt, modernity blurred the old borderline between the private and the public understood as 'political', and actually decisively replaced the ancestral private sphere with something preferably labelled as a 'sphere of intimacy', as well as the long-established public/political sphere with a new sphere of the social, whose content was regarded by the ancients as a private matter. See also: (Habermas 1992, p. 55).

[25] On alleged misconceptions of individuality as including the notion of dreams locked inside the body, or the impenetrability of the self: (Sloterdijk 2007, p. 263).

[26] Their metaphorical extensions are also many. See, for instance: (Beslay and Hakala 2007).

[27] Or '*Sphärentheorie*'. See, notably: (Doneda 2006, p. 67).

[28] Translatable as 'social sphere' (Alexy 2010, p. 236), or '*sphère de l'individualité*' (Robert 1977, p. 266).

[29] That can be translated as privacy, as 'a broader sphere of privacy' (Alexy 2010, p. 236), or as '*sphère du privé*' (Robert 1977, p. 266).

[30] Translatable as 'the innermost sphere', 'inviolable sphere of intimacy', or 'absolutely protected core are of private life' (Alexy 2010, p. 236), or '*sphère de l'intimité'* (Robert 1977, p. 266).

[31] Despite maintaining a sense of 'familiarity' and 'confidence', the English 'intimacy' eventually also acquired an extra meaning, related to sexual intercourse (Coronel Carcelén 2002, p. 19).

[32] Noting its importance for the Italian Frosini: (Martínez Martínez 2004, p. 205).

[33] See, interpreting the case law on the theory of the spheres as the basic German formulation of the right to privacy: (Riccardi 1983, p. 245).

als a *recht op eerbiediging van zijn persoonlijke levenssfeer*, which can be translated as a 'right to respect for their personal sphere of life'.[34]

The German theory of the spheres had been developed in the context of the German Federal Constitutional Court's doctrine on the existence of a general right to personality, or *das allgemeine Persönlichkeitsrecht*,[35] recognised on the basis of a joint reading of German constitutional provisions on the inviolability of human dignity,[36] and on the right to free development of personality.[37] The general right to personality represents what some have described as a fundamental freedom (Rigaux 1990, p. 16), encompassing a right to general freedom of action (Alexy 2010, p. 223), that some regard as a right to privacy (Krause 1965, p. 516). The notion of a general right to personality also generates some disorientation. This general right should not be confused with the notions of civil rights of personality or 'personality rights', sometimes portrayed as a sort of human rights recognised by civil law, and which the literature has also often linked to privacy discussions (Brügemeier 2010, p. 6). Although the legal category of personality rights is apposite in certain legal systems, such as the German[38] and the Austrian,[39] its pertinence to address privacy issues in other legal orders has been powerfully disputed.[40] In this sense, it has notably been argued that reliance on the notion of rights of personality creates normative and normalising effects, problematic for an understanding of privacy as freedom (Gutwirth 2002, p. 40).

The legal relevance of the distinction between what is private and what is public has been contested because of the complexities of distinguishing the private from the public (Turkington and Allen 1999, p. 8),[41] and but also because of the difficulties of ever identifying something that could be regarded as completely, hermetically private (Rigaux 1990, p. 16).[42] While some scholars defend that, despite the lack of general agreement on the dividing line between the private and the public, a division must exist (Blume 2002, p. 1), others have insisted on the fact that even in public contexts a certain privacy should be protected (Nissenbaum 2010),[43] and others prefer to replace the image of a division between the public and the private with the notion of a continuum in which privacy and publicity would be the ideal-typical

[34] Article 10 of the Dutch Constitution (since 1983).

[35] The recognition in Germany of a general right to personality has been linked to the traditionally limited protection granted through civil remedies (Rigaux 1997, pp. 139–140).

[36] Article 1(1) of the 1949 Fundamental Law of Bonn.

[37] Ibid. Article 2(1).

[38] In reality, Germany has witnessed many controversies on rights to personality, since the early nineteenth century (Strömholm 1967, p. 29).

[39] On this subject: (Universidad del País Vasco, Cuatrecases, and Mainstrat 2008, p. 3).

[40] See for instance: (De Schutter 1998, p. 58; Tulkens 2000, p. 28).

[41] Observing that 'for the vast majority of possible conflicts a clear distinction between private and public persons, documents, premises and activities cannot be made' (Strömholm 1967, p. 74).

[42] Concluding that should thus be privileged an idea of privacy emphasising the position occupied by the individual: (Rigaux 1990, p. 696). Echoing this reasoning: (Kayser 1995, p. 15).

[43] Nissenbaum actually refers to the existence of 'powerful moral reasons' obliging to limit the flow of private information in public (2010, p. 217).

endpoints (Nippert-Eng 2010, p. 4). Others still have designated the private/public boundary as an 'impossible distinction' (Derrida 1994, p. 146).[44]

But there is yet an additional important acceptation of the word privacy that is not grounded on any reading of the adjective private, and must be added to the above classification: privacy as control upon personal information.

2.1.2 (Re)defining Privacy in the US

The originality and significance of the conception of privacy as control upon personal information is best understood by taking into account the context of its historical surfacing. This account reveals the importance of the construction in the US of the so-called 'computers and privacy' issue.

2.1.2.1 US Privacy Before Computers

The expression 'right to privacy' entered the world of Anglo-American legal writing in 1890,[45] when US authors Samuel Warren and Louis Brandeis advanced its existence in a now famous article, unambiguously titled 'The right to privacy' (Warren and Brandeis 1890).[46] Warren and Brandeis build up their conception of a US right to privacy partially on English case law of the first half of the nineteenth century, which had indeed witnessed the use of the word privacy, even though only incidentally (Rigaux 1990, p. 13). They also claimed that the right had already found expression in the law of France, namely in the French *Loi relative à la presse* ('Law of the Press') of 11 May 1868, which prohibited the publication of facts related to the *'vie privée'* of individuals[47] unless the facts were already public, or were published with the individual's consent (Warren and Brandeis 1890, p. 214). Warren and Brandeis summarised the content of the right they supported equating it with the formula 'the right to be let alone' (Warren and Brandeis 1890, p. 214).[48]

In 1960, another US scholar, William L. Prosser, published an influential article in which it reviewed the acknowledgement of a privacy tort in common law since the publication of Warren and Brandeis's piece. Prosser described the recognition of four types of privacy tort: the intrusion upon a person's solitude or seclusion; the appropriation, for commercial purposes, of a person's name, likeness, or personality; the public disclosure of embarrassing private facts about a person; and the publicity that places a person in a false light in the public eye (Prosser 1960).[49]

---

[44] See also: (Gaston 2006, p. 11).

[45] See among others: (Strömholm 1967, p. 25; Rigaux 1992, p. 139).

[46] The article establishes the need for the legal recognition of the right to privacy by giving reasons largely centring around the practices of newspaper press. See also: (Pember 1972; Glancy 1979, p. 1).

[47] '*Toute publication dans un écrit périodique relative à un fait de la vie privée constitue une contravention punie d'amende de cinq cents francs*' (Warren and Brandeis 1890, p. 214).

[48] The formula is generally attributed to Thomas M. Cooley.

[49] See also: (Emerson 1979).

Privacy protection in the US was eventually developed not only through tort law, but also through constitutional law, which grants protection of individuals against the government. Although the US Constitution does not mention any right to privacy as such, various aspects of privacy are nowadays regarded as protected by the judicial interpretation of its provisions.[50] Brandeis himself became eventually judge of the US Supreme Court, from where he argued that the drafters of the US Constitution already recognised a right to be let alone in front of the State, and that this particular right was the widest and most esteemed of all.[51]

In 1965, the US Supreme Court explicitly declared that individuals have a constitutional right to privacy, located within the penumbras or zones of freedom created by an expansive interpretation of the US Bill of Rights.[52] From this perspective, the right to privacy can be regarded as a right to be free from government interference, growing out of the idea that there must be some freedoms beyond any State control, even in a democracy (McWhirter and Bible 1992, p. 33). This right to privacy would encompass both a negative or shielding protection, and a right to autonomy and self-determination (Pino 2002, p. 135) (for instance, by ensuring a right to abortion).[53]

By the mid 1960s, the term 'privacy' had thus acquired in the US two major meanings: on the one hand, it was used from the perspective of civil law as a synthetic reference to a system of torts (covering the intrusion in the private affairs of the person, the disclosure of private facts, or the use of a person's image); and, on the other hand, it appeared in the area of constitutional law as referring to the right for individuals to refuse interferences from public authorities (Pino 2002, p. 135).

2.1.2.2 Computers and Privacy

The linkage between computers and privacy as a matter worth of specific official attention, framed as the 'computers and privacy' issue, materialised as such in the US around 1965 (Westin 1970, p. 315). Electronic data processing machines had appeared in the US market a decade before (Westin and Baker 1972, p. 12). Prior to the 1960s, however, there had been practically no mention of any particular connec-

[50] Such as the First Amendment (freedom of speech, religion and association), the Third Amendment (which protects the privacy of the home by preventing the government from requiring soldiers to reside in people's homes), the Fourth Amendment (freedom from unreasonable searches and seizures), and the Fifth Amendment (privilege against self-incrimination), as well as, more occasionally, the Ninth Amendment, which states that the 'enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people'; due process and equal protection clauses also provide shields for privacy interests (Fisher 1995, p. 1172; Solove et al. 2006, pp. 33–34).

[51] See in particular Brandeis' dissenting opinion in the case *Olmstead v. United States* (277 U.S. 438).

[52] In the landmark 1965 judgment for *Griswold v. Connecticut* (318 U.S. 479), on the possibility to obtain birth control information. See: (McWhirter and Bible 1992, p. 59; Solove et al. 2006, p. 34).

[53] The landmark case on this subject is of 1973: *Roe v. Wade* (410 US 113, 1973). See: (Freedman 1987, p. 73).

tion between the deployment of computers and the endangerment of privacy (Westin 1970, p. 298). This was so even though the level of computerisation in organisations was already advancing quickly (Westin and Baker 1972, p. 12), and even if the late 1950s had already witnessed some occurrences of popular resistance to the processing of data related to individuals. For instance, religious and civil liberties organisations had raised protests against a proposal to introduce in a census[54] a question about religious preferences, arguing that it would have constituted a violation of the guarantees of freedom of religion and separation of Church and State, as well as a direct invasion of privacy of conscience (Westin 1970, p. 302). Discussions on the possible deployment of a universal personal identification system had also generated uproar (Westin 1970, p. 304). But it was only in the 1960s when computers began to be highlighted as a potentially important societal threat; more particularly, what was put forward as a threat was the automated processing of information on individuals that computers were capable of sustaining, and of trivialising.[55]

Computer specialists were the first to alert that computers' rapid and inexpensive processing of information, coupled with the increased availability of data to government agencies and private organisations, could carry with them some dangers (Westin 1970, p. 299),[56] notably to privacy. The first computer specialist forewarning of such a possible impact upon privacy might have been the president of a Californian company, Bernard S. Benson.[57] In 1961, Benson warned that more and more disparate information about individuals was being stored in computers without anybody noticing, but that the data could one day be fed into a single apparatus, leaving individual's privacy at the mercy 'of who or what controls the machine' (United Press International (UPI) 1961, p. 8).

In 1964, the American author Vance Packard[58] published *The Naked Society*, a book on the threats of then-emerging technologies, among which he pointed out the menaces of computerised filing. Packard echoed Benson's warnings on the machine's potential impact on individual privacy (1971, p. 49). In his view, however, emerging technologies appeared to endanger not only privacy, but also, and especially, numerous other rights such as 'the right to be different', 'the right to hope for tolerant forgiveness or overlooking of past foolishness, errors, humiliations, or minor sins' (what he described as the Christian notion of the possibility of redemption), or 'the right to make a fresh start' (Packard 1971, p. 23).

It was nonetheless the notion of privacy that increasingly gathered attention. By the beginning of the 1960s, debates had erupted over the impact on privacy of

[54] The 1960 US Federal Decennial Census.

[55] Noting that actually some security actors such as the US National Security Agency (NSA) had been at the forefront of research on computing: (Ceruzzi 2012, p. 38).

[56] Westin also refers to Richard W. Hamming, who had been involved since 1945 as a computer expert in the US research project for the production of an atomic bomb, and had warned since 1962 of some societal threats linked to the advent of computers.

[57] The Benson-Lehner Corporation, of Santa Monica, a company that developed data processing systems (United Press International (UPI) 1961, p. 8); also mentioned in: (Westin 1970, p. 299).

[58] Packard had acquired a relative notoriety in the US in 1957 with a book on the advertising industry, titled *The Hidden Persuaders* (Sawyer and Schechter 1968, p. 812).

various (then) new techniques and technologies—especially, electronic eavesdropping, psychological testing, and the use of polygraphs for lie detection. It was rather common in those days to insist on the idea that any new challenges for privacy were not being raised by vague scientific developments, or by 'esoteric new discoveries', but by very concrete (and increasingly pervasive) items embodying technological progress: for instance, battery-powered microphones, portable tape recorders, telephones that could be connected to a single main line, or high-resolution cameras (Ruebhausen 1970, p. xi).

In the context of this general preoccupation with the likely impact upon privacy of modern gadgets, in 1962 the Special Committee on Science and Law of the Association of the Bar of the City of New York[59] proposed to undertake a formal inquiry into the question (Ruebhausen 1970, p. ix). Noting how advances in electronic, optical, acoustic, and other sensing devices seemed to challenge individual privacy, the Special Committee on Science and Law placed the direction of this inquiry in the hands of Alan F. Westin, an expert on the topic of wire-tapping who had been writing about invasions of privacy for many years.[60] While the inquiry unfolded,[61] debates on privacy flourished across the US, and events and literature on the subject started to proliferate (Westin 1970, p. 312). Many of these manifestations were directly or indirectly attributable to the inquiry (Ruebhausen 1970, p. xi).

Formal support to incorporate the issue of computers into privacy debates arrived during this period: more precisely, in 1965, when a Subcommittee of US Congress, officially named the House Special Subcommittee on Invasion of Privacy of the Committee on Government Operations, chaired by Cornelius E. Gallagher,[62] added to the list of its agenda items the topic of computerisation (Westin 1970, p. 315). What brought the Subcommittee to that specific problem were various proposals envisaging the creation at federal level of 'data banks' centralising information about individuals already in the hands of federal authorities (Westin 1970, p. 316).[63] These proposals embodied the threat of massive quantities of information

[59] The Special Committee on Science and Law had been set up in 1959, following a previous experience in establishing a committee of lawyers to concern themselves with atomic energy (Ruebhausen 1970, p. viii).

[60] As well as Professor of Public Law and Government at Columbia University (Ruebhausen 1970, p. x).

[61] The research included a survey of the privacy-invading capacity of modern science, an exploration of the meaning of privacy, and an analysis of the interaction of the individual's claim to a private personality, society's need to acquire information and to control individual behaviour, as well as of new technology (Ruebhausen 1970, p. x).

[62] Gallagher had been particularly concerned with the impact upon privacy of the use of polygraphs for lie detection, and with personality tests being inflected upon employees and job applicants (Gallagher 1965).

[63] The proposals came from social scientists and government officials. The Executive Committee of the American Economics Association had recommended in 1959 to the US Social Science Research Council that it set up a committee to discuss the preservation and use of economic data. The committee issued a report on the subject in 1965, which it forwarded to the Bureau of the Budget for consideration (Sawyer and Schechter 1968, p. 812). A Budget Bureau consultant, Edgar S. Dunn, Jr., was asked to prepare a report on the matter. He recommended implementation of a national data centre. See: (Dunn 1967).

being easily stored and made readily available to the State for unknown purposes (Westin 1970, p. 312), generating much alarm in the media (Westin 1970, p. 317). In 1966, the Gallagher Subcommittee held hearings to discuss such proposals for federal data banks under the legend 'The Computer and Privacy' (Westin 1970, p. 319). The hearings eventually led to a series of recommendations to keep exploring the topic of 'privacy and the computer'.[64]

In 1967, the results of the research launched in 1962 by the Special Committee on Science and Law of the Association of the Bar of the City of New York were made public, in the form of a book titled *Privacy and Freedom*, by Alan F. Westin. Noting that computers had already been officially framed as a serious privacy problem,[65] Westin argued that, nonetheless, the thinking necessary to tackle the subject had still not been made accessible (1970, p. 323). His book was to contribute to fulfil this concrete gap by providing a new definition of 'privacy'.

Westin's definition supposedly applied to privacy in general, but had been unequivocally conceived in the light of the advent of computerisation. In his words: '(p)rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (1970, p. 7).[66] This account of privacy placed information at its very core. More particularly, for Westin the key feature of privacy consisted of the ability for individuals (or groups, or institutions) to exercise some control over the use of information about them (1970, p. 8).[67] As such, Westin's contribution was later to be described as a pioneering vision of privacy as information control, of a 'new privacy' (Grenier 1969, p. 253), of 'privacy of information' (Rössler 2004, p. 4), 'information privacy'[68] or 'informational privacy' (Turkington and Allen 1999, p. 75). The author, however, never used such phrases, and consistently referred to the conception of privacy he advanced and supported as being (just) privacy.

[64] Concrete recommended measures included the creation of a committee on problems of privacy and the computer within the American Federation of Information Processing Societies (AFIPS), which had been established in 1961 to disseminate knowledge in the field of information science, and the holding of a symposium on the subject (Westin 1970, p. 320).

[65] *Privacy and Freedom* granted attention to various techniques perceived as particularly privacy-invasive at the time, such as the use of polygraph and personality testing, labelled as methods of psychological surveillance (Westin 1970, p. 133), but included also a Chapter titled *The Revolution in Information Collection and Processing: Data Surveillance,* on the issue of privacy linked to computerisation (Westin 1970, p. 158).

[66] This is the definition authored by Westin that is quoted more often. He also provided some descriptions not fully consistent with it (for instance, referring to privacy as the voluntary and temporary withdrawal of a person from the general society through physical or psychological means (Westin 1970, p. 7)). Also noting these inconsistencies, see: (Rössler 2004, p. 16). Privacy is additionally depicted by Westin as a right of decision over one's private personality, and as a property right over personal information being processed (Westin 1970, p. 324).

[67] This idea was later further emphasised by Charles Fried: 'Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves' (Fried 1968, p. 482).

[68] Noting that 'information privacy' is often opposed to 'decisional privacy': (Solove et al. 2006, p. 1).

The move, interpreted by some as a call to extend the bounds of privacy protection in US law (Grenier 1969, p. 246), was presented by its author, rather, as a (re)discovery of the true sense of privacy. According to Westin, privacy had ancestral roots,[69] and constituted a functional necessity of democratic states (1970, p. 67). Efforts to limit surveillance in the name of privacy were portrayed as a central part of Western societies' struggle for liberty. He warned that surveillance was surreptitiously reaching the US 'as an accidental by-product of electronic data processing',[70] and constructed the insurance of privacy in relation to computers as a crucial element of free societies. This notion of (new/real) privacy as a critical element of modern freedom was further endorsed in another volume he co-authored a few years later, eloquently titled *Databanks in a Free Society: Computers, Record-Keeping and Privacy* (Westin and Baker 1972).

Reflections on individual control over personal information soon started to have a direct influence on the US legislator. In 1970 the US Congress adopted the Fair Credit Reporting Act,[71] for the protection against misuse of personal information held by Credit Reporting Agencies, which established procedures whereby individuals could take action to amend records about them.

In 1971, another authoritative book saw the light: Arthur R. Miller's *The Assault on Privacy* (Miller 1971). Miller further substantiated the link between computers and 'personal privacy' (1971, p. 18) by reviewing different threats of computer-driven intrusion.[72] Following Westin, he argued that the basic attribute of the right to privacy was 'the individual's ability to control the circulation of information relating to him' (Miller 1971, p. 40),[73] the problem with computers being, in Miller's view, that once 'personal information' has been stored, the individual to whom it refers (designated as 'the data subject') loses the capacity to control it (1971, p. 42). He stressed the increasing importance of computers for the setting up of governmental information systems (1971, p. 24),[74] and that individuals were most likely to lose control over their data to the benefit of governments.

---

[69] Westin argued simultaneously that claims to privacy derived from man's animal origins, and that the American approach to privacy had to be linked to a tradition of limiting public surveillance powers dating back to the ancient Greeks (1970, p. 7).

[70] The author described surveillance through the use of information as having been for centuries 'the conscious trademark of European authoritarian systems' (Westin 1970, p. 324).

[71] 15 U.S.C. § 1681 et sEq. Enacted as Title VI of Pub.L. 91–508, 84 Stat. 1114, enacted October 26, 1970, originally designed as an amendment to add a title VI to the Consumer Credit Protection Act, Pub.L. 90–321, 82 Stat. 146, enacted June 29, 1968.

[72] Miller identified as major privacy concerns: so-called 'decision-making by dossier', unrestricted transfer of information from one context to another, and surveillance conduct (see also: (Hixson 1987, p. 183)).

[73] He also observed that this attribute of control was in a way already present in the analysis by Warren and Brandeis.

[74] Miller also sensed that eventually computers would facilitate the provision of many services directly to individuals, commenting: 'it seems reasonable to envision some form of national computer "utility" providing a variety of data-processing services to everyone, perhaps through the medium of inexpensive home terminals such as touch-tone telephones or in conjunction with cable television' (1971, p. 33).

The publication of Miller's book is believed to have been the direct cause for a series of hearings celebrated in 1971 on the use of computers for data collection by another Subcommittee of US Congress, the Subcommittee on Constitutional Rights of the Senate (Hixson 1987, p. 207)[75] chaired by Sam J. Ervin, Jr. This Subcommittee had become gradually aware of governmental practices facilitating the accumulation of information,[76] and eventually decided to focus specifically on the exploration of privacy and automated information processing.[77]

2.1.2.3 Fair Information Principles

By the beginning of the 1970s, the depiction of computers as a major threat to *privacy* appeared to be accepted by a significant part of US population.[78] In 1972, the Secretary of the US Department of Health, Education and Welfare[79] established a Secretary's Advisory Committee on Automated Personal Data Systems, charged with analysing the harmful consequences that might result from such systems, and required to recommend safeguards to protect individuals. The Committee, which had among its members Arthur R. Miller, was chaired by a corporate researcher, Willis H. Ware.[80] During its investigation, the Committee explored recent developments in the area of the protection of individuals against 'automated personal data systems' as taking place in the US, but also elsewhere (Secretary's Advisory Committee on Automated Personal Data Systems 1973, sec. Appendix B: "Computers and Privacy": The Reaction in Other Countries). The Committee notably examined two legal instruments adopted in Europe, namely the Data Protection Act of the German federal state of Hesse, of 1970,[81] and the Swedish Data Law of 1973, which was by then still to enter into force. The Committee was also informed about related discussions taking place in France, and in the United Kingdom (UK).

The Secretary's Advisory Committee produced a report in 1973, under the title Records, Computers, and the Rights of Citizens (Secretary's Advisory Committee

[75] The Subcommittee had been established in 1955, and since then it had been interested in individual privacy, notably carrying out hearings on wire-tapping and government secrecy (Kaniuga-Golad 1979, p. 780).

[76] Sam J. Ervin, Jr. had been elected Chairman in 1961, and since then the Subcommittee concentrated on examining governmental infringement on individual privacy: its studies covered for instance the collection of personal information by the federal government through forms and questionnaires required of federal employees and job applicants (Westin 1970, p. 320). See also: (Ervin 1965).

[77] Kaniuga-Golad (1979) op. cit. 780.

[78] A national survey of public attitudes towards computers conducted in 1971 by the AFIPS jointly with *Time Magazine* showed that nearly 40% of the respondents considered the computer to be a real threat to privacy (Hondius 1975, p. 3); see also: (Harvard Law Review's Note 1968, p. 400).

[79] Elliot L. Richardson.

[80] Ware, of the RAND Corporation, had previously chaired a Task Force on Computer System Security (Task Force on Computer Security of the Defense Science Board 1970).

[81] The report also mentions the first activity report of the Data Protection Commissioner of the federal state of Hesse, published in 1972 (and the second one, published in 1973).

on Automated Personal Data Systems 1973).[82] This document put forward an unprecedentedly detailed description of how to address the 'privacy' concerns generated by the automated processing of information. Echoing Westin's analysis of privacy as primarily affected by the use of information about individuals, the report focused on the automated processing of 'personal data', a category defined as consisting of 'all data that describe anything about an individual',[83] and additionally referred to as 'identifiable information', or 'information about an individual in identifiable form'.[84]

In its report, the Secretary's Advisory Committee maintained that there existed many definitions of privacy, which all shared 'the common element that personal data are bound to be disclosed and that the data subject should have some hand in deciding the nature and extent of such disclosure' (Ware 1973, p. 3). Mirroring Westin's analysis, the Advisory Committee maintained that privacy had to be envisioned in terms of 'mutuality': it was necessary to make sure that both organisations holding personal data, on the one hand, and the data subject to which the data referred, on the other hand, shared control over it (Ware 1973, p. 3).[85] Safeguards for personal privacy based on such concept of mutuality required, the report explained, adherence by record-keeping organisations to some fundamental principles, all of them conceived as facets of a basic principle referred to as the principle of 'fair information practice' (Ware 1973, p. 7). The fundamental principles notably included the possibility for individuals to know which information about them has been recorded, and how it is used, as well as the capacity to correct information if necessary.[86] To implement these fundamental principles, organisations maintaining administrative personal data systems should comply with a series of obligations

[82] An explanatory report was published a month later by the Committee's Chairman: (Ware 1973).

[83] The report added: 'such as identifying characteristics, measurements, test scores; that evidence things done by or to an individual, such as records of financial transactions, medical treatment, or other services; or that afford a clear basis for inferring personal characteristics or things done by or to an individual, such as the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution' (Secretary's Advisory Committee on Automated Personal Data Systems 1973, Chap. IV "Recommended Safeguards for Administrative Personal Data Systems").

[84] See: Section 'A Redefinition of the Concept of Personal Privacy' (Secretary's Advisory Committee on Automated Personal Data Systems 1973, Chap. III "Safeguards for Privacy"). 'Personal information' and 'personal data' are presented as interchangeable also in a 1975 'glossary of frequently encountered terms' in the area of personal privacy (McCarthy 1975, p. 88).

[85] Any unbalance of control would generate information asymmetries, to be corrected; typically, the data subject is in a position of inferiority (Solove et al. 2006, p. 578).

[86] The principles identified by the Secretary's Advisory Committee were five: (1) no personal-data record-keeping system can be secret; (2) there must always be a way for individuals to find out what information about them is in the record and how it is used; (3) there must always be a way for individuals to prevent information obtained for one purpose from being used or made available for other purposes without their consent; (4) there must always be a way for individuals to correct or amend a record of identifiable information about them, and (5) any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use, and must take reasonable precaution to prevent any misuse.

(Ware 1973, p. 6); a public notice requirement should be approved, and individual data subjects should be granted a series of rights (Ware 1973, p. 7).

According to the 1973 Secretary's Advisory Committee's report, by then existed already a substantial number of US statutes and regulations that could be labelled as 'law of personal-data record keeping', such as the Fair Credit Reporting Act adopted in 1970.[87] Existing instruments, however, were portrayed as failing to configure a comprehensive and coherent body of law.[88] The main conclusion of the Committee's report was that it was consequently imperative to establish a code of 'fair information practice' for all automated personal data systems maintained by agencies of the federal government, or by organisations within reach of its authority (Ware 1973, p. 5).

2.1.2.4 Privacy Act

In January 1974, the President of the US, Richard Nixon, announced that before the end of the year the US government would 'make an historic beginning on the task of defining and protecting the right of personal privacy for every American' (Nixon 1974a).[89] In February 1974, he established in the White House a Domestic Council Committee on the Right of Privacy (Lane 2009, 190 ff). Chaired by the US Vice-President, Gerald Ford, the Committee on the Right of Privacy was instructed to examine the issue of the collection, storage, and use of personal data by the federal government, and to come up with recommendations, which could include legislative proposals, in a 4 months period (Nixon 1974b).[90] By then, however, the US Senate had already been investigating for almost a year various revelations on the illegal use of tape-recording systems by Nixon, in the context of the Watergate Scandal.[91] On 9 August 1974, Nixon resigned, and Ford became the President of the US.

On 31 December 1974,[92] the US Privacy Act was adopted, with the formal purpose of safeguarding individual privacy from the misuse of federal records,[93] and

[87] The report also mentioned the Federal Reports Act (44 U.S.C 3501–3511), and the Freedom of Information Act (5 U.S.C 552).

[88] Section 'Personal Privacy, Record Keeping, and the Law' (Secretary's Advisory Committee on Automated Personal Data Systems 1973, Chap. III "Safeguards for Privacy").

[89] Holding that '(m)odern information systems, data banks, credit records, mailing list abuses, electronic snooping, the collection of personal data for one purpose that may be used for another' had left millions of Americans deeply concerned with privacy, Nixon stated that time had come 'for a major initiative to define the nature and extent of the basic rights of privacy and to erect new safeguards to ensure that those rights are respected' (Nixon 1974a).

[90] Wiretapping and electronic surveillance were excluded from the Committee's mandate, officially because they were being studied by another Commission (McCarthy 1975, p. 86).

[91] The US Senate had set up a Select Committee on Presidential Campaign Activities, chaired by Sam J Ervin, Jr., particularly versed in privacy as attested by its prior inquiries.

[92] Effective since 27 September 1975.

[93] 'Records' were defined as 'any item, collection, or grouping of information about an individual' (Section 3 of the Privacy Act of 1974. The Act also included references to the category of 'identifiable personal information', which was not defined (see Section 2, point (b)(4) of the Privacy Act of 1974).

providing individuals access to them. The Act was substantially indebted to the 'fair information practice' doctrine as distilled by the Secretary's Advisory Committee in 1973. It provided safeguards for privacy by declining eight principles applicable to the use of records: the principles of openness, individual access (Kirby 1980, p. 7), individual participation, collection limitation, use limitation, disclosure limitation, information management, and accountability (Kirby 1980, p. 8). The Act applied to records in general, and thus not specifically to computerised records.

Despite its substantial link with the principles of 'fair information practices', the 1974 Privacy Act never mentions such phrase. It systematically refers to the safeguarding of privacy, described as a 'personal and fundamental right protected by the Constitution of the United States' directly affected by the collection, maintenance, use, and dissemination of personal information.[94] By doing so, the Privacy Act inscribed in US positive law the (then) fresh conceptualisation of privacy as 'new'/'information(al) privacy', and did so under the name of (just) privacy.[95]

This phenomenon, described as heralding a 'serious debasement' of the term 'privacy' (Clarke 2006), soon generated some ambiguity inside US law, especially concerning the interaction between the Privacy Act and other previously adopted acts such the Freedom of Information Act (FOIA) of 1966, which was also applicable to information possessed by federal agencies, and also alluded to privacy, but not in the same (modern, novel) sense.[96] The FOIA allowed for the disclosure of information controlled by the US Government, but provided for various exemptions, two of which were 'privacy' exemptions.[97]

At first, it was expected that the Privacy Act would set up an ad-hoc oversight board for the implementation of its provisions. Eventually, the Act only established a Privacy Protection Study Commission,[98] which in 1977 published a report on the problems of private and public sector record keeping systems. Titled *Personal Privacy in an Information* Society, the report advanced concrete policy recommendations (The Privacy Protection Study Commission 1977), implying major changes for private companies. The report was to be known as the final Privacy Protection Study Commission report, as the body was dissolved after its publication.

---

[94] See Section 2 (and in particular points (a)(1) and (a)(4) of the Congressional Findings) of the Privacy Act of 1974.

[95] Noting that the doctrine of 'fair information practices' was presented as privacy: (Piñar Mañas 2009, p. 86).

[96] Also echoing the confusion in the US literature and courts that is sometimes generated by the coexistence of different 'privacies' in US law: (Chemerinsky 2006, p. 650).

[97] A first concerned personnel and medical files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; the second, records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy (Solove et al. 2006, p. 529). See also: (Relyea 1980, p. 148).

[98] See Section 5(a)(1) of the Privacy Act of 1974. As originally drafted, the Privacy Act would have created a Federal Privacy Board to act as an oversight and enforcement mechanism (Rotenberg 2001, 39).

2.2 Privacy from an International Perspective

The writings by scholars such as Westin, the mentioned US Congress hearings, or the US Privacy Act of 1974 had significant repercussions, not only in the US,[99] but also in the rest of the world (Hondius 1975, p. 6). In Europe, awareness of the surveillance capacity of computers as a threat to society was gradually increasing (Flaherty 1989, p. 373), and an interest in the re-definition of privacy in the US was soon perceptible. The interest, however, generated initially primarily only tentative explorations of the linkage between computers and European approaches to 'privacy'.

2.2.1 Europe and the Search for (Modern) Privacy

Assessing the existence in Europe of privacy as a legal notion with any of the meanings described above engages a series of difficult challenges of comparative law. Revealingly, at the end of the 1960s this kind of comparative exercises was repeatedly undertaken both at national and international level, as the increasing use of the word privacy in the US to frame concerns related with modern information processing attracted more and more attention.

International law supplied some basic points of reference for discussions on privacy. The Universal Declaration of Human Rights (UDHR), proclaimed by the General Assembly of the United Nations (UN) in 1948, in Paris, establishes in the English version of its Article 12 that '(n)o one shall be subjected to arbitrary interference with his *privacy*,[100] family, home or correspondence, nor to attacks upon his honour and reputation'.[101] In its French version, Article 12 of the UDHR proscribes interferences with the *vie privée* of individuals; the Spanish version refers to the safeguarding of their *vida privada.*[102] The UDHR, however, does not define any of these notions. In 1966, the UN General Assembly adopted the International Covenant on Civil and Political Rights (ICCPR),[103] whose Article 17 mirrored the

[99] In 1977, the US Supreme Court extended constitutional privacy protection to information(al) privacy. Holding that the 'zone of privacy' protected by the Constitution encompasses the 'individual interest in avoiding disclosure of personal matters': *Whalen v. Roe*, 433 U.S. 425 (1977) (Solove et al. 2006, p. 34).

[100] Emphasis added.

[101] And that '(e)veryone has the right to the protection of the law against such interference or attacks' (Article 12 of the UDHR).

[102] English, French and Spanish have the status of official languages of the UN together with Arabic, Chinese (Mandarin), and Russian.

[103] Adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966.

content of Article 12 of the UDHR, repeating it almost word by word,[104] although still failing to provide any definition of privacy, *vie privée* or *vida privada.*[105]

The European Convention on Human Rights (ECHR),[106] signed on 4 November 1950, builds upon the UDHR, but, insofar as privacy is concerned, does not sustain exactly the same terminological approach. Although it mirrors Article 12 of the UDHR in its Article 8, the English version of the ECHR does not refer to any privacy, using instead the notion of 'respect for private life'; in addition, in contrast to the UDHR, it does not include any mention of 'honour' and 'reputation' (Velu 1973, p. 42), words allegedly dismissed by the drafters of the ECHR due to their vagueness (Ruiz Miguel 1992, p. 99). The French version of the ECHR—the only other authentic linguistic version—prohibited interferences with the *respect de la vie privée.* Eventually, the European Court of Human Rights' case law on Article 8 of the ECHR had a powerful influence on securing a wide understanding of the notion of 'respect for private life'/*respect de la vie privée* across Europe, but in the 1960s its case law had yet to develop in that direction.

Another example of the convoluted relations between the terms privacy, private life and *vie privée* in international law can be found in the American Convention on Human Rights signed in San José, Costa Rica, on 22 November 1969, by the Organization of American States.[107] The American Convention on Human Rights represents the most important human rights instrument of the inter-American system (De Schutter 2010, p. 27). It recognises in the English version of its Article 11 a right to privacy that prohibits interferences with the 'private life' of individuals.[108] The French version of the same article, however, establishes not a right to *vie privée*, but to the '*protection de l'honneur et de la dignité de la personne*' (translatable as 'the protection of honour and dignity of the person'), which forbids interferences with the *vie privée* of individuals.[109]

---

[104] Article 17 of the ICCPR reads: '(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks' (cf. Article 12 of the UDHR: the word 'unlawful' has been added).

[105] In 1988 was adopted General Comment No. 16 on Article 17 ICCPR, referring to an explicit mandate to regulate by law the gathering and holding of personal information on computers, databanks and other devices (Human Rights Committee, General Comment No. 16 (Twenty-third session, 1988), in *Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies*, UN Doc. HRI/GEN/1/Rev.1 at 21 (1994)).

[106] Formally the Convention for the Protection of Human Rights and Fundamental Freedoms.

[107] Headquartered in Washington, D.C. (US).

[108] Article 11 of the American Convention on Human Rights: 'Right to Privacy: (1) Everyone has the right to have his honor respected and his dignity recognized; (2) No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation; (3) Everyone has the right to the protection of the law against such interference or attacks'.

[109] A similar phenomenon can be perceived in other official linguistic versions. The official languages of the Organization of American States are English, Spanish, Portuguese, and French. See also: (Rigaux 2000, p. 126 and 128).

2.2.1.1 The 1967 Nordic Conference

By the end of the 1960s, the International Commission of Jurists (ICJ), a non-governmental organisation devoted to the promotion of human rights, started to consider necessary to investigate more deeply the notion of privacy, and its safeguarding. In May 1967, the organisation's Swedish section hosted in Stockholm a special meeting on the topic, named the Nordic Conference of Jurists on the Right to Respect for Privacy. An extensive working paper with a comparative study specifically prepared for the Conference noted that there were major terminological discrepancies in the field, and that many countries appeared to provide what some regarded as 'privacy protection' through different notions and mechanisms (Strömholm 1967, p. 21).

The comparative study was signed by the Swedish lawyer Stig Strömholm, who noted that although the facts giving rise to privacy-related legal concerns where similar everywhere, there were notable differences in the approaches and techniques of the Anglo-American, German and French lawyers (1967, p. 20). Strömholm identified as major reference in Continental Europe, as a concept akin to privacy, the notion of rights of the personality, which was presented as paradigmatic of the German approach (1967, p. 21), and somehow also of the French perspective. He classified perceived commonalities between the US notion of 'invasions of privacy' and violations of rights of the personality into three basic categories: intrusions into an area that people have an interest in keeping for themselves; collecting material about somebody by any method felt to be unfair, and using material about a person for some specific purpose (1967, p. 60).

Strömholm's study embraced the use of the term privacy only reluctantly, noting that it was 'practically inevitable in a paper written in English', and emphasised it should not be read as implying the adoption *a priori* of 'the Anglo-American way or ways or defining the subject under consideration' (1967, p. 21). Despite these warnings, the Nordic Conference went ahead with a discussion focused on privacy, using this term as encompassing also related legal notions developed in Europe under other names, and eventually concluded by encouraging the adoption of laws establishing a general right to privacy. Thus, *a posteriori* it endorsed the framing of the subject through English terminology. The right to privacy, in the view of the participants to the Conference, had not only to be explicitly recognised in law, but also broadly configured[110] in the light of technological developments, ensuring in particular the protection against interferences with correspondence, misuse of private communications, or disclosure of information received in circumstances of professional secrecy (A. Warren and Dearnley 2005, p. 240). No particular reference was made to computers as a possibly relevant technological development in the area.

[110] The Nordic Conference's final declaration included under the notion of 'privacy' Prosser's torts, but went beyond them (Michael 1994, p. 13).

2.2.1.2 From Recording Techniques to Computers

Shortly afterwards, the UN similarly resolved to start exploring the possible impact of technological progress on the protection of the individual. In 1968, an International Conference of Human Rights organised by the UN in Tehran[111] recommended that UN institutions scrutinise the problems with regard to respect for privacy in view of the evolution of recording techniques.[112] As a follow up, the UN General Assembly asked the UN Secretary General to undertake a study of the problems for the respect of human rights, and especially the respect of privacy, in the light of general technical and technological advances.[113] In 1970, discussions emerged also under the auspices of the UN Educational, Scientific and Cultural Organisation (UNESCO), which convened an expert meeting to examine the impact of developments in science and technology believed to have created a threat to the individual's right to privacy and related human rights and fundamental freedoms.[114] Subsequently, UNESCO entrusted the ICJ with the preparation of a (new) comparative international investigation (ICJ 1972, p. 417).

Still in 1970, the British Section of the ICJ, called JUSTICE, published its own study on privacy. Titled *Privacy and the Law*, it incorporated a whole appendix specifically on the issue of *Computers and Privacy*, which described the threat that computerisation might pose to the privacy rights of individuals (Littman and Carter Rusk 1970). This report by JUSTICE and Westin's *Privacy and Freedom*[115] became the two main sources used by the ICJ to complete the study for UNESCO (ICJ 1972, p. 417).

The final ICJ study, published in 1972, noted that the Nordic Conference of 1967 had failed to discuss with enough detail what was already considered by then, in the view of many, the most serious of all threats to privacy: the collection, storage and disclosure of personal data using computers (1972, p. 420). According to the ICJ, this particular threat required not laws on a general right to privacy, but rather ad-hoc legislation, which should guarantee the right of individuals to know which data about them are being processed, and to have them rectified if necessary, as well as strict control

[111] International Conference on Human Rights, 22 April to 13 May 1968.

[112] Resolution XI concerning human rights and scientific and technological developments, adopted by the International Conference on 12 May 1968, para 2. The International Conference culminated in the adoption of a general Proclamation stating that scientific discoveries and technological advances could endanger the rights and freedoms of individuals (Proclamation of Teheran, Final Act of the International Conference on Human Rights, Teheran, 22 April to 13 May 1968, United Nations Document A/CONF. 32/41, paragraph 18).

[113] General Assembly of the United Nations, *Resolution 2450 (XXIII) on Human rights and scientific and technological developments*, 1748th plenary meeting, 19.12.1968 (see especially paragraph 1(a)). Paragraph 1(c) also mentions uses of electronics that may affect the rights of the person, and the limits which should be placed on such uses in a democratic society.

[114] Developments such as the miniaturisation of recording devices, wiretapping and eavesdropping mechanisms and similar devices (Commission on Human Rights of the United Nations Economic and Social Council 1970, p. 23).

[115] The 1972 report classified the nature of technical threats to privacy using Westin's tripartite division into physical surveillance, psychological surveillance, and data surveillance.

of the access to information, compliance with a general purpose limitation principle, and the existence of an authority analogous to an ombudsman with technical means allowing it to monitor the observance of the rules, and which would have the power to receive and examine complaints (1972, p. 578).

The study thus illustrated two notable changes in thinking about privacy, compared to the outcome of the 1967 Nordic Conference. Five years before, the Nordic Conference had not even considered computers among the (many) technological developments that (dangerously) threatened the right to privacy. Now, the ICJ was unambiguously marking out computerisation as the major threat. In 1967, the organisation had backed up the recognition in law of a broadly constructed general right to privacy. In 1972, it explicitly advocated instead for the adoption of specific regulation focusing on the automated processing of data about individuals, to encompass a series of individual rights over data concerning them, obligations upon those using the data, and a monitoring authority. In its search for a modern approach to the protection of privacy, the ICJ had encountered privacy as (shared) control over the use of personal data, and had embraced this notion as the concrete desired target.[116]

The spread of the influence of (post-Westin) privacy as control upon personal information was manifest not only in Europe. Canada, for instance, also supported similar investigations. In 1968 the Ontario Law Reform Commission, which had been attempting to determine the nature of the problems 'in the area referred to compendiously as the "right to privacy"' (Ontario Law Reform Commission 1968, p. 1) taking into account both the results of the 1967 Nordic Conference and of Westin's research, published a report indicating 'a serious and growing concern by distinguished jurists, scholars and men in public life throughout the Commonwealth and throughout the world with the grave threat that is posed to all free men and democratic institutions by modern technology and well-intentioned government and commercial practices that expose the individual to public and institutional scrutiny' (1968, p. 1). Therefore, it recommended a federal-level study to be undertaken by a Task Force (Ontario Law Reform Commission 1968, p. 3).

In 1971 a Canadian Task Force on *Privacy and Computers*[117] was thus asked to consider the rights and values of the individual clustering around the notion of privacy, and to examine the effects on these rights and values of computerised information systems containing personal data about identifiable individuals.[118] In its final report, the Canadian Task Force suggested among other things that a commissioner

[116] The UN adopted Guidelines for the Regulation of Computerized Personal Data Files in 1990 (adopted by the General Assembly Resolution 45/95 of 14 December 1990).

[117] Emphasis added.

[118] In this sense: (Secretary's Advisory Committee on Automated Personal Data Systems 1973, sec. Appendix B "Computers and Privacy": The Reaction in Other Countries). In May 1970 a conference jointly sponsored by the federal Departments of Justice and Communications and the Canadian Information Processing Society was held at Queen's University on the topic 'Computers: Privacy and Freedom of Information'; the Task Force had its origin in the deliberations of that conference (Task Force established by the Department of Communications and Department of Justice (Canada) 1972, p. 2).

or ombudsman be established, that carefully prepared test cases be brought before the courts, and that the operation of government data systems be made to serve as model (Task Force established by the Department of Communications and Department of Justice (Canada) 1972).[119] The Canadian Task Force also concluded that privacy was in a sense too limited a word to encompass all the concerns created by massive and pervasive information systems, and observed that it was used in part as a synonym for political grievances about the use of information systems by institutions to enhance their power to the potential detriment of individuals, and for fears that information systems may be used to manipulate individuals or enforce conformity (Task Force established by the Department of Communications and Department of Justice (Canada) 1972, p. 183).

2.2.1.3 The United Kingdom and the Quest for Privacy

In their famous 1890 article putting forward the existence of a right to privacy, Warren and Brandeis had argued that the right's roots could be traced back, *inter alia*, to references to privacy in English and French law. The possible existence of a right to privacy in the United Kingdom was nevertheless vividly debated during various decades. In England and Wales, the common law did not develop a general right to privacy, nor did Parliament introduce one. In the absence of a general law on privacy, the common law developed a fact-specific approach, protecting privacy through, for instance, the law of confidentiality, or breach of confidence (Lord Neuberger of Abbotsbury 2012, p. vii). The protection granted was typically described as arising 'almost by accident, as an incidental effect of a variety of laws established for other purposes' (ICJ 1972, p. 457), unable to evolve towards a more general privacy protection (Colvin and Cooper 2009, p. 17). During various decades, the idea of privacy as an encompassing notion was viewed as a theoretical concept merely adopted by writers under American influence (Strömholm 1967, p. 26).

Echoing the conclusions of the 1967 Nordic Conference, the report prepared in 1970 by the British Section of the ICJ, JUSTICE, had championed the recognition of a general right of privacy in the UK (Littman and Carter Rusk 1970). JUSTICE had also drafted a Privacy Bill, officially submitted in November 1969 by Brian Walden, and which similarly called for the creation of a general right of privacy, as well for the establishment of civil remedies for some infringements (Warren and Dearnley 2005, p. 241).[120] Actually, by the beginning of the 1970s there were in the UK multiple privacy-related bills: also in 1969, a Data Surveillance Bill was put forward,[121] calling for the registration of computerised personal data banks;

[119] See also: (Secretary's Advisory Committee on Automated Personal Data Systems 1973, sec. Appendix B "Computers and Privacy": The Reaction in Other Countries).

[120] See also: (Younger 1972, p. 1).

[121] By Kenneth Baker in the House of Commons, and by Lord Windlesham in the House of Lords.

and an unsuccessful Control of Personal Information Bill was introduced by Leslie Huckfield in 1971.

As a response to the 1970 JUSTICE report and Walden's Privacy Bill,[122] the UK government announced its intention to carry out a detailed examination of the subject of privacy. In May 1970 a Committee on Privacy was appointed for this purpose, with Sir Kenneth Younger as chairman. Younger's Committee on Privacy (as it was generally known) was however not particularly interested in the possible recognition of a general right of privacy by statute.[123] The Committee, noting that privacy had been generating a large literature in the US, and that the aspect that had attracted by far the most attention was the 'privacy' of computerised personal information (Younger 1972, p. 3), decided to concentrate on discussing the use of computers for the processing of information, and more concretely their use in the private sector—even if the subject had not been listed among its tasks. As Younger's Committee on Privacy was exploring these issues, a Workshop on the Data Bank Society[124] brought to London selected US experts,[125] and highlighted the need for legislative control of computerised data banks (Younger 1972, p. 179).

Younger's Committee on Privacy published its final report ('the Younger Report') in 1972. The report formulated a series of principles for the computerised handling of personal information[126] to be taken into account by the data-processing industry, and urged the industry to voluntarily adopt them as a code of good practice. The report also recommended the setting up of a Standing Committee to consider the use of computers and their impact on individuals (Jay 2007, p. 5).

In 1973, after debate in Parliament of the Younger Report, the UK government announced that it would respond with the publication of a White Paper.[127] 1973 was also the year when the UK joined the European Economic Community (EEC). In the end, the UK government published not one but two White Papers, both in 1975,[128] and subsequently set up a Data Protection Committee[129] under the chairmanship of

[122] More precisely, during the second reading debate in the House of Commons of the Right of Privacy Bill introduced by Brian Walden (Younger 1972, p. 1).

[123] Its final report stated it was relevant to note that England had traditionally not chosen that way as its way to protect the main democratic rights of citizens (Younger 1972, p. 10).

[124] Organised in November 1970 under the title 'Privacy, Computers and You'.

[125] Including Alan F. Westin and Cornelius E. Gallagher (Hanlon 1970).

[126] The principles were: the purpose of holding data should be determined; there should only be authorised access to data; there should be minimum holdings of data for specified purposes; persons in statistical surveys should not be identified; subject access to data should be given; there should be security precautions for data; there should be security procedures for personal data; data should only be held for limited relevant periods; data should be accurate and up to date; and any value judgments should be coded (Warren and Dearnley 2005, p. 242).

[127] The Younger report had concrete repercussions in the UK 1974 Consumer Credit Act, which included provisions to allow individuals to access the information related to them, and a mechanism to facilitate the expression of disagreement.

[128] One titled *Computers and Privacy* (CMND 6353), announcing the government's intention to consider legislation and its supplement, *Computers: Safeguards for Privacy* (CMND 6354), dealing with computer use in the public sector.

[129] Describing this Data Protection Committee as a 'forerunner of a permanent authority': (Flaherty 1979, p. 53).

Sir Norman Lindop,[130] which in 1976 was commissioned to look at the operation of computer systems in the public and private sectors, and to advise on the most suitable means of ensuring appropriate safeguards for the protection of individuals (Jay 2007, p. 5).

The Report of the Committee on Data Protection ('the Lindop Report') was issued in 1978 (Committee on Data Protection 1978). Targeting the insurance of both privacy[131] and data protection, it recommended the adoption of legislation covering the public and private sectors, the setting up of an independent authority to ensure supervision (Jay 2007, p. 5), and the mandatory registration of some computer users in order to process data (Critchell-Ward and Landsborough-McDonald 2007, p. 518). The Lindop report failed to generate any concrete response. It was only in 1984, after the Council of Europe approved a legally binding Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), that the UK passed its first Data Protection Act (Roos 2003, p. 260). And it was only in 1998, with the enactment of a Human Rights Act that brought about the integration of Article 8 of the ECHR into UK law, that the protection of privacy in the UK definitely entered a new phase.[132]

2.2.2 Privacy in Other Words?

The UK was not alone in Europe reflecting on privacy and the regulation of data processing. Other European countries were carrying out similar investigations precisely using the same term, privacy. And still others chose instead other legal framings to consider fairly similar issues.

2.2.2.1 Privacy in Other Languages

If the salience of privacy in US discourse strongly contributed to the notion's prominence in English-speaking countries and organisations (Bygrave 2010, p. 167), its hold was also soon perceptible in non-English speaking countries. Some of them even integrated into their own languages the word privacy as such.

One of the first languages to adopt the word 'privacy' from English in the context of a reflection on the legal reaction to the advent of computers was Dutch. The phenomenon occurred in the two European countries where Dutch is an official language, namely Belgium and the Netherlands. In 1970, an International Colloquium

[130] Initially Younger was to be made Chairman of this Committee, but he died in May 1976 (Warren and Dearnley 2005, p. 259).

[131] As noted also in (Critchell-Ward and Landsborough-McDonald 2007, p. 518).

[132] In what has been described as a 'seismic shift' (Lord Neuberger of Abbotsbury 2012, p. vii), or a sort of 'mini-revolution' (O' Cinneide et al. 2006, p. 554).

took place in Brussels, celebrated with support of the Council of Europe.[133] Its title had three linguistic versions: English, with 'Privacy and Human Rights'; French, as in 'Vie privée *et droits de l'homme*'; and Dutch, which referred to 'Privacy[134] *en Rechten van de Mens'*.[135] The reference in Dutch to 'privacy' illustrates an accelerating integration of this term in Dutch-speaking literature as a loan word.

In the Netherlands, the announcement of a General Census in 1970 functioned as a catalyst for a massive sense of anxiety among the population on the collection and use of personal information (De Graaf 1987, p. 1). In 1971, a Governmental Committee on Privacy and Personal Registers was established under the chairmanship of Thijmen Koopmans, and entrusted to explore the issue. The Koopmans Committee published in January 1974 an Interim Report titled *Privacy en persoonsregistratie,* where it proposed the adoption of data protection legislation for the public and the private sector (Hondius 1975, p. 39).[136] As in the UK, the adoption of concrete rules suffered nevertheless a great delay, materialising only in 1989 (Overkleeft-Verburg 1995, p. 571). In the meantime, a major revision of the Dutch Constitution inscribed in it in 1983 a general *recht op eerbiediging van zijn persoonlijke levenssfeer* ('right to respect of the personal sphere of life')[137] accompanied by a mandate to legislate on its protection in relation to the recording and dissemination of personal data,[138] and on the rights to access to and rectification of such data.[139] None of these provisions used the (by now also Dutch)[140] term *privacy*, which is nonetheless still widely employed by the doctrine (Koops 2011, p. 168). In Belgium, the Constitution enshrines since 1994 a right to the protection of what its Dutch version refers to as *privé-leven*; *Privatleben* in the German version, and *vie privée* in the French one.[141]

2.2.2.2 Vie Privée or Libertés?

According to Warren and Brandeis, the right to privacy had found an expression in the law of France already in the nineteenth century, taking the shape of the notion

[133] The Conference took place from 30 September to 3 October 1970. It was organised jointly by the Belgian government and the Council of Europe, and was the third edition of a series of Conferences supported since 1965 by the Council of Europe on different aspects of the protection of human rights, with special focus on the application of the ECHR. For the presentations in English: (Robertson 1973).

[134] Emphasis added.

[135] The event devoted special attention to computers and Westin's definition of privacy (Ganshof van der Meersch 1974, p. 5 and 147 (contribution by R. V. Jones)).

[136] The Committee's final report was published in 1976.

[137] Article 10(1) of the Dutch Constitution.

[138] Ibid. Article 10(2).

[139] Ibid. Article 10(3).

[140] (Van Hoof et al. 2001, p. 765).

[141] Article 22 of the Belgian Constitution (adopted in three official languages: Dutch, French and German). The terminological choice was possibly linked to the fact that previously the judiciary had established the direct applicability of Article 8 of the ECHR on the right to respect for private life (Electronic Privacy Information Center (EPIC) and Privacy International (PI) 2007, p. 262).

of *vie privée*.[142] The idiom *vie privée* had as a matter of fact made a remarked appearance in France already in 1819, when the essayist Pierre Paul Royer-Collard, discussing a proposal on crimes committed by the press at the *Chambre des députés*, alluded to the *vie privée* as something to be protected by a fortress, walled against attacks by the outside world.[143]

The English privacy and the French *vie privée* are configured as equivalent in a number of international instruments, such as the UDHR, even if in 1950 the ECHR privileged 'private life' as its corresponding idiom.

Debates on the notion of *vie privée* were particularly vivid in France by the beginning of the 1970s.[144] The Act of 17 July 1970[145] introduced a new Article 9(1) into the French Civil Code, explicitly stating that everybody has the right to respect for their privacy/private life ('*Chacun a droit au respect de sa vie privée*').[146] This provision, which added up to existing mechanisms guaranteeing related protection,[147] did not define the meaning of *vie privée*, which nonetheless eventually came to be described as covering both the protection of individuals' *intimité* ('intimacy')[148] and autonomy (in the sense of the legitimacy for individuals to be free to live their lives as they wish with a minimum of external interferences) (Détraigne and Escoffier 2009, p. 14).[149] This broad understanding of the notion of *vie privée* found further support in Article 8 of the ECHR, ratified by France in 1974,[150] and in its reading by the ECtHR.

Also in the early 1970s, France experienced a key change in its constitutional case law. In 1971, the Constitutional Council *(Conseil constitutionnel*) recognised a whole body of binding constitutional rules (the so-called *bloc de*

[142] See above, Sect. 2.2.1 of this chapter.

[143] That mention was however somehow fortuitous (Rigaux 1992, p. 139), as Royer-Collard's main concern was to promote freedom of press (Brügemeier 2010, p. 12).

[144] Illustrating interest on the subject since the end of the 1960s: (Malherbe 1968, 1968).

[145] With the Law 70/643 of 17 July 1970.

[146] The provision reads: '*Chacun a droit au respect de sa vie privée. Les juges peuvent sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé'*.

[147] Such as the *loi du 29 juillet 1881 sur la liberté de la presse*, or Article 1382 of Code Civil (Nerson 1971, p. 739).

[148] Respect for private life concerns most importantly intimacy if one focuses on the second paragraph, describing the nature of interference with private life that can lead to judicial measures (aiming at '*empêcher ou faire cesser une atteinte à l'intimité de la vie privée'* (Abravanel-Jolly 2005, p. 63).

[149] *Conclusions Cabanes prises dans CA Paris, 7ème chambre, 15 mai 1970* (Détraigne and Escoffier 2009, p. 14). The duality of *vie privée* is sometimes portrayed in terms of a distinction between the *secret de la vie privée* (or the secrecy of privacy) and the *liberté de la vie privée* (or privacy as freedom). See for instance: (Kayser 1995, p. 11; Abravanel-Jolly 2005, p. 63).

[150] France ratified the ECHR on 3 May 1974, through the authorisation given by loi n° 73–1227 of 31 December 1973. In France, the ECHR has supremacy over national legislation (Brügemeier 2010, p. 16).

constitutionnalité),[151] which notably includes the 1789 Declaration of the Rights of Man and of the Citizen, and in which are regarded as constitutionally entrenched a series of *libertés publiques*, or public freedoms. Individual freedom, a constitutionally protected freedom, came eventually to be considered as including protection for the *vie privée* of individuals,[152] and the *Conseil constitutionnel* judged that the notion has its foundation in Article 2 of the Declaration of 1789, which mentions freedom as one (as a matter of fact, the first) of the natural and imprescriptible rights of citizens (Sudre 2005, p. 404).

When at the beginning of the 1970s French authorities started to inquiry on the impact of emerging technologies, and in particular computers, on the rights of the individual, they framed the issue in terms of a relationship between *l'informatique* (computers) and *libertés* (or public freedoms).[153]

2.2.2.3 Swedish as a Language Without Privacy

Other European countries also addressed around the same time similar issues, in not dissimilar ways, through still different terminological lenses. A clear example of this phenomenon is the Swedish case.

In Sweden, computerization of the public sector began comparatively soon, in the early 1960s (Söderlind 2009, p. 270), and was relatively well advanced by the end of the decade. Popular uproar followed the announcement of a census in 1969, as part of the population realised that the gathering of information had been specifically designed to facilitate automated data processing. In reaction to these concerns, the Swedish Government entrusted the task of studying the problems of computerised record keeping to an official commission already in place,[154] the Parliamentary Commission on Publicity and Secrecy of Official Documents.[155]

The Swedish Parliamentary Commission on Publicity and Secrecy of Official Documents published in June 1972 its own report on computerised record keeping. Its title was *Data och integritet*, and it rapidly came to be known in English-speaking circles as 'Computers and Privacy':[156] the Swedish word *data* specifically denoted information automatically processed (Hondius 1975, p. 84), which seemingly justified its translation as 'computers', and Swedish appeared to lack

[151] *Décision n° 71–44 DC1, relative à une loi "complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association"*. See also: (Brügemeier 2010, p. 15).

[152] This position was explicitly adopted by the French *Conseil constitutionnel* decades later, in its decision 99–416 DC of 23 July 1999, by declaring that *'la liberté proclamée par (l'article 2 de la Déclaration des droits de l'homme et du citoyen) implique le respect de la vie privée'* (Détraigne and Escoffier 2009, p. 14).

[153] See Chap. 3, Sect. 3.4, of this book.

[154] (Secretary's Advisory Committee on Automated Personal Data Systems 1973, sec. Appendix B "Computers and Privacy": The Reaction in Other Countries).

[155] Offentlighets- och sekretesslagstiftningskommittén.

[156] See, for instance: (Flaherty 1979, p. 112; Working Party for Information Security and Privacy (WPISP) 2011, p. 74).

any other word closer to 'privacy' than *integritet*—which explains why *integritet* and privacy are often regarded as synonymous (Flaherty 1989, p. 104), despite the fact that *integritet* is sometimes also translated into English as 'personal integrity' (Flaherty 1989, p. 105). In its report, the Parliamentary Commission highlighted the importance of *integritet* as a problem of trust and confidence between the State and citizens, while emphasising the benefits of the use of computer technology in public administration (Söderlind 2009, p. 272). Swedish discourse surrounding the regulation of data processing still focuses nowadays on the notion of *integritetsskydd* ('protection of (personal) integrity') (Bygrave 2002, p. 322).

2.3 Summary

This chapter has carried out an exploration of the reputedly elusive notion of privacy. It has underlined that there exist many conceptions of the notion, embodying multiple entanglements with concepts such as freedom, dignity, or personality, but also one vision standing out due to its relatively clear content, and its substantive concern with the processing of information about individuals: privacy re-defined as information(al) privacy, a modern, post-Westin notion which can be summarised as 'control upon personal information'. This meaning of the word was distilled by the US literature since the end of the 1960s in the context of discussions on the development of computers and the protection of individual freedom, and which led to the development in the US of the doctrine of 'fair information practices'. The doctrine stressed the need to impose obligations on those who process information about individuals, but also to grant a set of rights for the individuals whose information is processed—in particular, a right to know about such processing, and to rectify inaccuracies. At its core was the possibility for individuals to know what information about them was held by other parties.

The 1974 Privacy Act consolidated a connection between the word privacy and the doctrine of 'fair information practices', and notably the principle of individual access, as well as the principle of use limitation. The Privacy Act applies to information about individuals stored in records held by some public authorities (federal agencies), regardless of whether it is processed electronically or not. Access to such information had been also previously regulated through the lens of freedom of information. From that perspective, privacy had traditionally played a different role: it functioned as a possible ground justifying refusal of access. The appearance of redefined notion of privacy by the end of the 1960s, thus, added an extra layer of meaning to the word, but did not replace previous understandings.

As those developments unfolded, a number of European countries were also attempting to refine their own approach to the protection of the individual in the light of technological progress. Explorations of the notion of privacy soon surfaced in this context, which gradually circumscribed threats linked to technological progress to the advent of computers. International organisations such as the ICJ documented the absence of the recognition of a general right to privacy in international law, and

called for its enshrinement. Eventually, however, the ICJ dropped this ambition, and refocused its efforts towards the promotion of instruments specifically dealing with the regulation of the automated processing of data.

Similarly, the UK destined much effort to discussing the possible acknowledgement of the existence of a right to privacy, but from there, and through the concrete consideration of the issue of computers, shifted towards deliberations on statutes on what it started calling by the mid-1970s 'data protection'. The usage of the word privacy in the US did not find an exact equivalent in the UK, or elsewhere in Europe.

This chapter has shown that the increasing global popularity of the term 'privacy' led to some non-Anglophone European countries to borrow the word and use it in the context of their own investigations on the protection of individuals and data processing. In others countries, nonetheless, debates turned around different terminology, as the French *libertés*, or the Swedish *integritet.* France and Sweden were precisely, together with Germany, among the first European countries to adopt special legal instruments to regulate the processing of personal data in order to reinforce the legal protection of individuals.

References

Abravanel-Jolly, Sabine. 2005. *La protection du secret en droit des personnes et de la famille*. Paris: Defrénois.

Alexy, Robert. 2010. *A Theory of Constitutional Rights (originally published 2002)*. Oxford: Oxford University Press.

Arendt, Hanna. 1998. *The Human Condition*. Chicago: The University of Chicago Press.

Bendich, Albert M. 1996. Privacy, poverty and the constitution. *California Law Review* 54 (2): 407–442.

Bennett, Colin J. 1992. *Regulating Privacy: Data protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.

Bennett, Colin J., and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: The MIT Press.

Bennett, Tony, Lawrence Grossberg, and Meaghan Morris. 2001. *New Keywords: A Revised Vocabulary of Culture and Society*. Oxford: Blackwell.

Beslay, Laurent, and Hannu Hakala. 2007. Digital territory: Bubbles. In *European visions for the knowledge age: A quest for new horizons in the information society*, ed. Paul T. Kidd, 69–78. Cheshire Henbury.

Bioy, Xavier. 2006. L'identité de la personne devant le Conseil constitutionnel. *Revue Française de Droit constitutionnel* 1 (65): 73–95.

Blume, Peter. 2002. *Protection of Informational Privacy*. Copenhaguen: DJØF.

Brügemeier, Gert. 2010. Protection of personality rights in the law of delict/torts in Europe: Mapping out paradigms. In *Personality Rights in European Tort Law*, eds. Gert Brüggemeier, Aurelia Colombi Ciacchi, and Patrick O'Callaghan, 5–37. Cambridge: Cambridge University Press.

Bureau de la Terminologie du Conseil de l'Europe. 1995. *Lexique Anglais-Français (principalement juridique)*. Strasbourg: Conseil de l'Europe.

Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

Bygrave, Lee A. 2010. Privacy and data protection in an international perspective. *Scandinavian Studies in Law* 56:165–200.

Ceruzzi, Paul E. 2012. *Computing: A Concise History*. London: The MIT Press.

Chemerinsky, Erwin. 2006. Rediscovering Brandeis's right to privacy. *Brandeis Law Journal* 45 (July): 643–657.

Clarke, Roger. 2006. What's 'Privacy'? Workshop at the Australian Law Reform Commission. http://www.rogerclarke.com/DV/Privacy.html. Accessed March 10, 2013.

Colvin, Madeleine, and Jonathan Cooper, eds. 2009. *Human Rights in the Investigation and Prosecution of Crime*. New York: Oxford University Press.

Commission on Human Rights of the United Nations Economic and Social Council. 1970. Human rights and scientific and technological developments: Report of the secretary-general (Addendum 1). E/CN.4/102.

Committee on Data Protection. 1978. *Report of the committee on data protection (chairman Sir Norman Lindop)"*. London: Her Majesty's Stationery Office.

Coronel Carcelén, Felipe Francisco. 2002. *La protección del derecho a la vida privada en Internet y otros medios de comunicación electrónicos*. Santiago: Pontificia Universidad Católica de Chile.

Critchell-Ward, Ann, and Kara Landsborough-McDonald. 2007. Data protection law in the European Union and the United Kingdom. *Comparative Law Yearbook of International Business* 29:515–578.

De Graaf, Frederik. 1987. *Privacy en Persoonsgegevens: Het Ontwerp van Wet Persoonsregistraties*. Lelystad: Koninklijke Vermande.

De Hert, Paul, and Serge Gutwirth. 2003. Privacy concerns. In Security and privacy for the citizen in the post-September 11 digital age: A prospective overview, report to the European Parliament Committee on Citizen's Freedoms and Rights, Justice and Home Affairs (LIBE), Report EUR 20823 EN, ed. European Commission Joint Research Centre, Institute For Prospective Technological Studies.

De Schutter, Olivier. 1998. La vie privée entre droit de la personnalité et liberté. In Privacy: Seminarie Egmontpaleis 26 & 27 Nov. 1998, 46–84, Brussel: Minister van Buitenlandse Zaken.

De Schutter, Olivier. 2010. *International Human Rights Law*. Cambridge: Cambridge University Press.

Derrida, Jacques. 1994. *Politiques de l'amitié*. Paris: Éditions Galilée.

Détraigne, Yves, and Anne-Marie Escoffier. 2009. Rapport d'information fait au nom de la Commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et de l'administration générale par le Groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques. Paris: Sénat.

Dictionnaire Gaffiot Latin-Français. 1934. Hachette.

Doneda, Danilo. 2006. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.

Duby, Georges. 1999. Ouverture. In *Histoire de la vie privée : 2. De l'Europe féodale à la renaissance*, eds. Philippe Ariès and Georges Duby. Paris: Editions du Seuil.

Dunn Jr., Edgar S. 1967. The idea of a national data center and the issue of personal privacy. *The American Statistician* 21 (1): 21–27.

Edelman, Bernard. 1999. *La personne en danger*. Paris: Presses Universitaires de France.

Electronic Privacy Information Center (EPIC), and Privacy International (PI). 2007. Privacy & Human Rights 2006: An international survey of privacy laws and developments. Washington, D.C. and London: EPIC / PI.

Elias, Norbert. 1991. *La société des individus*. Paris: Librairie Arthème Fayard.

Emerson, Thomas I. 1979. The right of privacy and freedom of the press. *Harvard Civil Rights-Civil Liberties Law Review* 14 (2): 329–360.

Ervin Jr., Sam J. 1965. Why Senate hearings on psychological tests in government. *American Psychologist* 20 (11): 879–880.

Fisher, Louis. 1995. *Constitutional Rights: Civil Rights and Civil Liberties*. 2nd ed. New York: McGraw-Hill.

Flaherty, David H. 1979. *Privacy and Government Data Banks: An International Perspective*. London: Mansell.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press.

Freedman, Warren. 1987. *The right of privacy in the Computer Age*. London: Quorum Books.
Fried, Charles. 1968. Privacy. *The Yale Law Journal* 77 (3): 475–493.
Frowein, Jochen A. 1985. Art. 8 Privat- und Familienleben. In *Europäische MenschenRechstKonvention: EMRK-Kommentar*, eds. Jochen A. Frowein and Wolfgang Peukert. Kehl am Rhein: Engel.
Gallagher, Cornelius E. 1965. Why House hearings on invasion of privacy. *American Psychologist* 20 (11): 881–882.
Ganshof van der Meersch, Walter J. 1974. Privacy en Rechten van de Mens: 3e Internationaal Colloquium over het Europees Verdrag tot Bescherming van de Rechten van de Mens [1970-Brussel]. Acco.
Gaston, Sean. 2006. *Derrida and Disinterest*. London: Continuum.
Gavison, Ruth. 1980. Privacy and the limits of law. *The Yale Law Journal* 89 (3): 421–471.
Glancy, Dorothy J. 1979. The invention of the right to privacy. *Arizona Law Review* 1 (21): 1–29.
Grenier Jr., Edward J. 1969. Computers and privacy: A proposal for self-regulation. In Proceedings of the first ACM symposium on problems in the optimization of data communications systems.
Gutwirth, Serge. 2002. *Privacy and the Information Age*. Oxford: Rowman & Littlefield.
Habermas, Jürgen. 1992. *The Structural Transformation of the Public Sphere*. Cambridge: Polity.
Halimi, Gisèle. 1992. *La cause des femmes précédé de Le temps des malentendus*. Paris: Gallimard.
Hanlon, Joseph. 1970. British workshop airs data bank problems (9 December 1970). Computer world: The newsweekly for the computer community: 2.
Hansson, Mats G. 2008. *The Private Sphere: An Emotional Territory and its Agent*. Dordrecht: Springer.
Harvard Law Review's Note. 1968. Privacy and efficient government: Proposals for a national data center. *Harvard Law Review* 82 (2): 400–417.
Hildebrandt, Mireille. 2006. Privacy and identity. In *Privacy and the Criminal Law*, eds. Erik Claes, Anthony Duff, and Serge Gutwirth, 43–58. Antwerp: Intersentia.
Hixson, Richard F. 1987. *Privacy in a Public Society: Human Rights in Conflict*. Oxford: Oxford University Press.
Hondius, Frits W. 1975. *Emerging Data Protection in Europe*. Amsterdam: North-Holland.
International Commission of Jurists (ICJ). 1972. The protection of privacy. *International Social Science Journal* XXIV (3): 414–602.
Jay, Rosemary. 2007. *Data Protection Law and Practice*. London: Sweet & Maxwell.
Kahn, Jonathan. 2003. Privacy as a legal principle of identity maintenance. *Seton Hall Law Review* 33 (2): 371–410.
Kaniuga-Golad, Ludmila. 1979. Federal legislative proposals for the protection of privacy. *Fordham Urban Law Journal* 8 (4): 773–817.
Kayser, Pierre. 1995. *La protection de la vie privée par le droit : Protection du secret de la vie privée (3e édition)*. *Aix-en-Provence*. Marseille: Presses Universitaires d'Aix-Marseille.
Kirby, Michael Donald. 1980. International guidelines to protect privacy in trans border data flows. Australian & New Zealand Association for the Advancement of Science, Jubilee Congress, Adelaide, 15 May 1980.
Koops, Bert-Jaap. 2011. The evolution of privacy law and policy in the Netherlands. *Journal of Comparative Policy Analysis* 13 (2): 165–179.
Krause, Harry D. 1965. The right to privacy in Germany—Pointers for American legislation? *Duke Law Journal* 3:481–530.
Lane, Frederick S. 2009. *American Privacy: The 400-year History of our Most Contested Right*. Boston: Beacon Press.
Lefebvre-Teillard, Anne. 2003. Personne. In *Dictionnaire de la culture juridique*, eds. Denis Alland and Stéphane Rials. Paris: Quadrige/Lamy-PUF.
Littman, M., and P. F. Carter Rusk, eds. 1970. Privacy and the law: A report by the British section of the International Commission of Justice. Stevens.
Locke, John. 1998. *Identité et différence: L'invention de la conscience II* (edited, translated and commented by Etienne Balibar). Paris: Seuil.

Lord Neuberger of Abbotsbury. 2012. Foreword. In *Privacy Injunctions and the Media*, ed. Iain Goldrein, vii–viii. Oxford: Hart.
Luhmann, Niklas. 1998. *Love as Passion: The Codification of Intimacy*. Stanford: Stanford University Press.
Malherbe, Jean. 1968. *La vie privée et le droit moderne*. Paris: Enseignement et perfectionnement techniques.
Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.
McCarthy, Alice. 1975. Privacy—A perspective. In Privacy, a public concern: A resource document (Proceedings of a seminar, Washington, DC, December 1974), ed. Kent S. Larsen. Council of State Governments.
McWhirter, Darien A., and Jon D. Bible. 1992. *Privacy as a Constitutional Right: Sex, drugs and the Right to Life*. New York: Quorum Books.
Mekas, Jonas. 2010. I had nowhere to go 1947–50/1991 (Excerpt). In *Jonas Mekas,* eds. Museum Ludwig and Serpentine Gallery, 18–21. Koenig Books.
Michael, James. 1994. *Privacy and human rights: An international and comparative study, with special reference to developments in information technology*. Aldershot: Dartmouth/UNESCO.
Miller, Arthur R. 1971. *The Assault on Privacy: Computers, Data Banks and Dossiers*. Ann Arbor: University of Michigan Press.
Nerson, Roger. 1971. La protection de la vie privée en droit positif français. *Revue Internationale de Droit Comparé* 23 (4): 737–764.
Nippert-Eng, Christena. 2010. *Islands of Privacy*. Chicago: The University of Chicago Press.
Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
Nixon, Richard M. 1974a. State of the union message of 30 January 1974.
Nixon, Richard M. 1974b. Radio address about the American Right of Privacy of 23 February 1974.
O' Cinneide, Colm, Myriam Hunter-Henin, and Jörg Fedke. 2006. 'Privacy' in J. M. Smits (ed), (Edward Elgar 2006). In *Elgar Encyclopedia of Comparative Law*, ed. J. M. Smits, 554–565. Cheltenham: Edward Elgar.
Onions, Charles Talbut. 1966. *The Oxford Dictionary of English Etymology*. Oxford: Clarendon Press.
Ontario Law Reform Commission. 1968. Report on protection of privacy in Ontario (1968). Toronto.
Overkleeft-Verburg, Margriet. 1995. De Wet Persoonsregistraties: Norm, Toepassing en Evaluatie. Katholieke Universiteit Brabant.
Packard, Vance. 1971. *The Naked Society (originally published in 1964)*. Harmondsworth: Penguin Books.
Pember, Don R. 1972. *Privacy and the Press: The Law, the Mass Media, and the First Amendment*. Seattle: University of Washington Press.
Pérez Luño, Antonio Enrique. 2010. *Derechos Humanos, Estado de Derecho y Constitución*. 10th ed. Madrid: Tecnos.
Piñar Mañas, José Luis. 2009. Protección de datos: Origen, situación actual y retos de futuro. In *El derecho a la autodeterminación informativa*, eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 81–179. Madrid: Fundación Coloquio Jurídico Europeo.
Pino, Giorgio. 2002. Giudizi di valore e dottrine civilistiche: Il caso dei diritti della personalità. *Diritti & Questioni Pubbliche* 2 (agosto): 132–173.
Pino, Giorgio. 2006. Il diritto all'identità personale ieri e oggi: Informazione, mercato, dati personali. In *Libera circolazione e protezione dei dati personali*, ed. Rocco Panetta. Milano: Giuffrè.
Prosser, William L. 1960. Privacy. *California Law Review* 48 (3): 383–423.
Relyea, Harold C. 1980. Freedom of information, privacy, and official secrecy: The evolution of federal government information policy concepts. *Social Indicators Research* 7:137–156.
Riccardi, J. Lee. 1983. The German Federal Data Protection Act of 1977: Protecting the right to privacy? *Boston College International & Comparative Law Review* VI (1): 243–271.

Ricoeur, Paul. 1990. *Soi-même comme un autre*. Paris: Seuil.
Rigaux, François. 1990. *La protection de la vie privée et des autres biens de la personnalité*. Bruxelles: Bruylant.
Rigaux, François. 1992. *La vie privée, une liberté parmi les autres?* Bruxelles: Larcier.
Rigaux, François. 1997. *La loi des juges*. Paris: Éditions Odile Jacob.
Rigaux, François. 2000. L'individu, sujet ou objet de la société de l'information. In *La protection de la vie privée dans la société de l'information : Tome 1*, ed. Pierre Tabatoni, 122–137. Paris: Presses Universitaires de France.
Robert, Jacques. 1977. *Libertés publiques*. Paris: Montchrestien.
Robertson, A. H. 1973. *Privacy and human rights: Papers by experts on an issue of growing importance given under the auspices of the European convention on human rights*. Manchester: Manchester University Press.
Rodotà, Stefano. 2009. *La vita e le regole: Tra diritto e non diritto*. Milano: Feltrinelli.
Roos, Anneliese. 2003. *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study*. University of South Africa.
Rössler, Beate. 2004. Privacies: An overview. In *Privacies*, ed. Beate Rössler, 1–18. Stanford: Stanford University Press.
Rotenberg, Marc. 2001. *The Privacy Law Sourcebook 2001: United States Law, International Law, and Recent Developments*. Washington, D.C.: Electronic Privacy Information Center (EPIC).
Ruebhausen, Oscar M. 1970. Foreword. In *Privacy and freedom*, ed. Alan F. Westin, i–xvi. New York: Atheneum.
Ruiz Miguel, Carlos. 1992. *La configuración constitucional del derecho a la intimidad*. Madrid: Universidad Complutense de Madrid.
Sawyer, Jack, and Howard Schechter. 1968. Computers, privacy, and the national data center: The responsibility of social scientists. *American Psychologist* 23 (11): 810–818.
Schoeman, Ferdinand David. 2008. *Privacy and Social Freedom*. Cambridge: Cambridge University Press.
Scott, Joan W., and Debra Keates, eds. 2005. *Going Public: Feminism and the Shifting Boundaries of the Private Sphere*. Urbana: University of Illinois Press.
Secretary's Advisory Committee on Automated Personal Data Systems. 1973. Records, Computers, and the Rights of Citizens.
Serfaty-Garzon, Perla. 2003. *Chez soi : Les territoires de l'intimité*. Paris: Armand Colin.
Sloterdijk, Peter. 2007. *Spheres Volume I: Bubbles—Microspherology*. Los Angeles: Semiotext(e).
Söderlind, Åsa. 2009. Personlig Integritet som Informationspolitik: Debatt och Diskussion i Samband med Tillkomsten av datalag (1973:289). Institutionen Biblioteks- och informationsvetenskap/Bibliotekshögskolan, Högskolan i Borås och Göteborgs universitet.
Sofsky, Wolfgang. 2009. *Defensa de lo privado: Una apología*. Valencia: Pre-textos.
Solove, Daniel J. 2006, January. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (3): 477–564.
Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge: Harvard University Press.
Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz. 2006. *Information Privacy Law*. 2nd ed. New York: Aspen.
Strömholm, Stig. 1967. *Right of Privacy and Rights of the Personality: A Comparative Survey*. Stockholm: Boktryckeri AB Thule.
Stuart Mill, John. 1948. *On Liberty (originally published in 1859)*. London: Watts & Co.
Sudre, Frédéric. 2005. *Droit européen et international des droits de l'homme*. 7th ed. Paris: Presses Universitaires de France.
Task Force established by the Department of Communications and Department of Justice (Canada). 1972. *Privacy and Computers*. Ottawa: Information Canada.
Task Force on Computer Security of the Defense Science Board. 1970. Security controls for computer systems.
The Privacy Protection Study Commission. 1977. Personal privacy in an information society.
Thomas, Yan. 2011. *Les opérations du droit*. Paris: Seuil/Gallimard.

Tulkens, Françoise. 2000. La liberté d'expression et d'information dans une société démocratique et le droit au respect de la vie privée au regard de la Convention européenne des Droits de l'homme : Regards croisés sur les Articles 8 et 10 de la Convention dans la jurisprudence de la Cour européenne des Droits de l'homme. In *In Rapports de la Conférence sur la liberté d'expression et le droit au respect de la vie privée du 23 septembre 1999*. Strasbourg: Conseil de l'Europe.

Turkington, Richard C., and Anita L. Allen. 1999. *Privacy Law: Cases and Materials*. St. Paul: West Group.

United Press International (UPI). 1961. Electronic brain 'Peril' to Liberty. *Sarasota Journal*, p. 8 April 17.

Universidad del País Vasco, Cuatrecases, and Mainstrat. 2008. Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality: Annex 3. JLS/2007/C4/028. European Commission, Directorate General Justice and Home Affairs, Directorate C: Civil Justice, Rights and Citizenship.

Van Hoof, D. C., D. Verbruggen, and C. H. Stoll, eds. 2001. *Elsevier's Legal Dictionary*. Amsterdam: Elsevier.

Velu, Jacques. 1973. The European Convention on Human Rights and the right to respect for private life, the home and communication. In *Privacy and human rights*, ed. A. H. Robertson, 12–128. Manchester: The University Press.

Ware, Willis H. 1973. Records, Computers and the Rights of Citizens. The Rand Paper Series 1973.

Warren, Samuel, and Louis Brandeis. 1890. The right to privacy. *Harvard Law Review* 4 (5): 193–220.

Warren, Adam, and James Dearnley. 2005. Data protection legislation in the United Kingdom. *Information. Communication & Society* 8 (2): 238–263.

Westin, Alan F. 1970. *Privacy and Freedom, (originally published in 1967)*. New York: Atheneum.

Westin, Alan F., and Michael A. Baker. 1972. *Databanks in a Free Society: Computers, Record-keeping and Privacy*. New York: Quadrangle Books.

Working Party for Information Security and Privacy (WPISP). 2011. The evolving privacy landscape: 30 years after the OECD Privacy Guidelines, Directorate for Science, Technology and Industry—Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG (2010) 6/FINAL, 6.4.2011". DSTI/ICCP/REG (2010) 6/FINAL.

Wright Mills, Charles. 2000. *The Power Elite (originally published in 1956)*. Oxford: Oxford University Press.

Younger, Kenneth. 1972. *Report of the Committee on Privacy*. London: Her Majesty's Stationery Office.

Chapter 3
The Surfacing of National Norms on Data Processing in Europe

> *Intanto, questo,—egli mi dice:—che fuori della legge e fuori di quelle particolarità, liete o triste che sieno, pero cui noi siamo noi, caro signor Pascal, non è possibile vivere.*
> *Ma io gli faccio osservare che non sono affatto rientrato né nella legge, né nelle mie particolarità. Mia moglie è moglie di Pomino, e io non saprei proprio che dire ch'io mi sia.*
> *("Well, there's this, for one thing," says he. "Your story shows that outside the law of the land, and apart from those little happenings, painful or pleasant as they may be, which make us each what we are, life, my dear Pascal, life is impossible." Whereupon I point out to him that I fail to see how that can be; for I have not regularized my life whether in relation to the law of the land or in relation to my private affairs. My wife is the wife of Pomino, and I'm not quite sure who I am myself!' (translated by Arthur Livingston: (Luigi Pirandello 1923)).*
>
> (Pirandello 1904)

In the 1970s started to see the light in various European countries different provisions regulating the automated processing of data. They basically took two distinct forms: they were either ad-hoc acts, or constitutional-level provisions. Each of them advanced a particular legal approach to the protection of individuals in the face of automated data processing, typically enacting varied terminology and contrasted standpoints on the rights and freedoms involved. Only a few mentioned something directly translatable as data protection, and only a few were associated to anything resembling privacy.

This chapter examines this initial materialisation of provisions on automated data processing in European national legal orders, exploring their diversity to better understand their linkage with the eventual emergence of a right to the protection of personal data as a fundamental right of the European Union (EU). It does not pretend to offer a complete overview of existing or past regulations in any Member State, but rather to single out elements that later became instrumental in the construal of European personal data protection.

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law,* Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_3,

3.1 Pioneering Ad-Hoc Acts

The German federal state of Hesse, Sweden, Germany and France were the first to go ahead in Europe with the adoption of legal acts applicable to the processing of information related to individuals. Their acts can be regarded as opening up a first period or wave of regulating activity, a wave starting in 1970 and ending in 1981 with the adoption of Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), which subsequently became a main reference for all European legislators, influencing the drafting of later laws.[1]

3.1.1 German Federal State of Hesse

The first legal instrument bearing the German name of *Datenschutz,* a word that would later be translated into English as 'data protection', was approved in October 1970 by the German federal state of Hesse, one of the states constituting Germany: it was the *Hessische Datenschutzgesetz*, or Data Protection Act of Hesse.[2] The Act regulated the use of information stored on the Land's governmental files. It provided a series of safeguards that were considered not adequately described by previously existing German legal terms, such as *Datensicherung* (data security) or *Datensicherheit* (also translatable as data security) (Bygrave 2002, p. 22).

The *Hessische Datenschutzgesetz* followed chronologically the official setting up of public data processing facilities in the federal state of Hesse, which had been particularly active in promoting the automated processing by public authorities of information on individuals.[3] Other German federal states had set up similar data processing facilities by simultaneously adopting a number of clauses protecting the rights of individuals.[4] In Hesse, instead, rules on data protection were laid down only afterwards, in a separate instrument (Hondius 1975, p. 36). As a result, this instrument became the first separate law laying down rules of general application for data protection. Its adoption was preceded by a careful study of previous similar experiences around the world, and especially in the US, a country that the *Hessische*

[1] Corresponding to what Spiros Simitis envisions as the first phase of the development of data protection: (Simitis 2006, pp. 108–117).

[2] Hessische Datenschutzgesetz vom 7. Oktober 1970 GVBl. II 300-10, published at Wiesbaden, 12 October 1970, in *Gesetz-und Verordnungsblatt für das Land Hessen* [Laws and Regulations Journal], Part I, No. 41. For an early unofficial English translation published by OECD, see: (Dammann et al. 1977, p. 113).

[3] Hessian Act on data processing centres of Land and Communes, of 16 December 1969. The federal state of Hesse had started collecting information on individuals and storing it in computers by the mid-1960s (Simitis 2010, 1995).

[4] Notably, Bavaria (Act of 12 October 1970) and Baden-Württemberg (Act of 17 November 1970). The first law of this kind had been adopted by the federal state of Schleswig-Holstein in 1968 (Hondius 1975, p. 35).

Datenschutzgesetz's drafters regarded as the prevailing information source (Simitis 2010, p. 1995).[5]

The Hesse Data Protection Act applied exclusively to the public sector; more concretely, to the authorities of the Land and the organisations depending of the Land when using records prepared for the purpose of automatic data processing, storing data, or obtaining results from such data.[6] The Act defined *Datenschutz* as the obligation for records, data and results to be obtained, transmitted and stored in such a way that they cannot be consulted, altered, extracted or destroyed by an unauthorised person.[7] It also laid down norms of data confidentiality in the form of rules of conduct to be observed by the authorities in charge, and by the computer personnel (Hondius 1975, p. 5). The Hesse Data Protection Act additionally contained provisions on the rights of individuals concerned by the information stored, who may notably demand the rectification of incorrect data.[8] Moreover, institutional controls were introduced in the form of a *Datenschutzbeauftragter* (Data Protection Commissioner), charged with supervising compliance with the law, and, generally, with the mission of observing the effects of computerisation on the balance of power between the various public organs of the Land (Hondius 1975, p. 36).

The word *Datenschutz* was successful in Germany, and all over Europe. All European languages have by now integrated it through direct calques similar to the English 'data protection'. The German *Daten* is however, strictly speaking, not fully equivalent to the English 'data'. The English word has been traditionally used to refer in general to any given piece of information,[9] or to information known or assumed as facts (very much like the French *donnée(s),* or the Dutch *gegeven(s)*, for instance). With the advent of computer technology, these words (data, *données, gegeven(s)*) acquired a new specific meaning in the emerging field, and started to be used also concretely denoting the information operated upon by computers (Hondius 1975, p. 84). The German language, on the contrary, had not being relying on the term *Daten* before computerisation. It espoused the word precisely in such context. *Daten* was thus not understood at the time as referring to just any data, but specifically to the data that computers processed (Hondius 1975, p. 84).

In 1974, another German Land, Rhineland-Palatinate, adopted a data protection act: the *Gesetz gegen missbräuchlich Datennutzung* (Act Against Misuse of Data).[10] Despite not being formally named as a 'data protection act', the Act referred to *Datenschutz* in its very first article. It defined it as the provisions insuring that electronic data processing, in particular in public databases, did not interfere with

[5] Spiros Simitis was one of the drafters of the first Hessian Data Protection Act (Gassmann 2010, p. 6).

[6] Section 1 of 1970 Hesse Data Protection Act.

[7] Ibid. Sect. 2.

[8] Section 4 of 1970 Hesse Data Protection Act.

[9] The etymological origin of 'data', found in the plural of the Latin word *datum*, echoes this interpretation of data as a *given* piece of information.

[10] Adopted on 24 January 1974.

the legitimate interests of natural or legal persons.[11] *Datenschutz* was thus the main object of these provisions, which did not make any explicit link to any other legal notion except with the wide formula of the legitimate interests of persons.[12] As the term refers to a series of rules applying to the processing of information to individuals, it was later considered, in some circumstances, as synonymous with (informational) privacy.[13]

3.1.2 Sweden

The first national law regulating automated data processing ever to see the light in Europe was the Swedish *Datalag* (Data Act) of 11 May 1973,[14] which entered into force on 1 July 1973. The *Datalag* was the direct outcome of the public concern generated by the public census of 1969, and the subsequent publication in 1972 of the report titled *Data och integritet* by the Swedish Parliamentary Commission on Publicity and Secrecy of Official Documents.[15] In the 1972 report, the Swedish Parliamentary Commission highlighted the importance of *integritet* as a problem of trust and confidence between the State and citizens, while emphasising the benefits of the use of computer technology in public administration (Söderlind 2009, p. 272). It proposed the adoption of a special statute, as well as the establishment of a new authority, the *Datainspektionen* or Data Inspection Board, to be responsible for the implementation of the legislation, and for the protection of individuals (Söderlind 2009, p. 272).

The pioneering role played by Sweden in this field can be explained by a number of reasons. Since the 1940s, it had been developing a system of identification through personal identification numbers, which, in the light of increasingly rapid computerisation public administration, caused concern due to its capacity to rapidly integrate information a priori decentralised (Burkert 1999, p. 48). Perhaps more importantly, Sweden has traditionally granted an extraordinary relevance to openness, and, concretely, to the principle of public access (*offentlighetsprincip*) (Steele 2002, p. 19).

[11] Article 1(1) of the 1970 Hesse Data Protection Act: 'Bei der elektronischen Datenverarbeitung, insbesondere bei der Einrichtung von Datenbanken, durch Behördern oder Einrichtungen des Landes sowie der Aufsicht des Landes unterstehende Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts oder in deren Auftrag, ist Vorsorge dafür zu treffen, dass durch die Erfassung, Speicherung, Nutzung öder Löschung von Daten schutzwürdige Belange von natürlichen oder juristischen Personen sowie von nichtrechtsfähigen Vereinigungen nicht beeinträchtigt oder verletzt werden (Datenschutz)'.

[12] Soon after the adoption of the Hesse Data Protection Act, other German federal states considered some similar bills, a few of them bearing references to the notion of *Privatsphäre* (Hondius 1975, p. 36), but the word was absent from the 1970 Hessian Act.

[13] See, for instance: (Von Beseler and Wüstefeld 1986, p. 1299; Van Hoof et al. 2001, p. 765).

[14] (Sweden) Data Act given in the Palace of Stockholm, May 11, 1973, SFS 1973: 289. For an English Translation for the Council of Europe (EXP/Prot. Priv. (73) 5): (Dammann et al. 1977, p. 129). The Datalag was mainly drafted by Jan Freese (Gassmann 2010, p. 6).

[15] See Chap. 2, Sect. 2.2.2.3, of this book.

Sweden guarantees public access to official documents since the adoption of the Freedom of Press Act of 1766, and the currently in force 1949 Freedom of the Press Act is regarded as an integral component of the Swedish Constitution. The *offentlighetsprincip* essentially provides that all information and documents held by public institutions must be available to all members of the public. There are nevertheless a series of exemptions, and the right of access to official documents might be restricted if necessary, inter alia, for the protection of personal integrity (*personlig integritet*) of individuals. In 1965, the Swedish Supreme Administrative Court held that the principle that every citizen should have access to official documents also encompassed computer-stored information (International Commission of Jurists (ICJ) 1972, p. 447).

The 1973 Data Act had as its official purpose to prevent undue invasions *i registrerads personliga integritet*, or of the personal integrity of the person whose data were registered in data banks. The Data Act used the term *data*, but delimited its scope of application through the notions of *upplysning* and *personuppgift*,[16] translatable as information and personal information (Dammann et al. 1977, p. 130). It applied to information held in machine-readable form both by public and private parties.[17] Following the suggestions of the Parliamentary Commission, it created a Data Inspection Board to regulate the collection and dissemination of identifiable personal data in computerised form. The setting up of independent boards was also a relatively well-established Swedish approach. Sweden had been responsible for the invention of the modern notion of the ombudsman (originally a Swedish word), and had acquired the practice of establishing specific ombudsmen to deal with concrete policy issues (ICJ 1972, p. 446).

Pursuant to the 1973 Data Act, it became generally unlawful to start or maintain any personal data register in machine-readable form without permission from the Data Inspection Board.[18] The Act contained few material provisions on when and how data could be processed; instead, it required for each computerised personal data register a prior permission from the Data Inspection Board, which then issued tailor-made conditions for the register (Öman 2004, p. 390). The *Datainspektionen* was soon problematically overloaded by applications for licenses (Söderlind 2009, p. 273), but the idea of establishing a mechanism of central registration of personal data processing information, together with a licensing procedure, was successfully exported (Frosini 1984, p. 7). It quickly became highly influential across Europe and for the European Economic Community (EEC), even if Sweden became a Member State only much later, in 1995.

3.1.3 Germany

The first country that was a Member State of the European Communities (EC) when adopting an ad-hoc statute on the processing of data was Germany. The German

[16] Section 1 of 1973 *Datalag*.

[17] Describing this as a unique feature: (Burkert 1999, p. 47).

[18] See, for instance: (Flaherty 1979, p. 112).

Parliament (*Bundestag*) had expressed since the late 1960s its support for the adoption of a general federal act on this subject (Riccardi 1983, p. 248). In 1971, the German Federal Government asked a research group[19] to study the structure of a possible federal law, and the research group launched its inquiry drawing heavily on the writings of US authors such as Alan F. Westin[20] and Arthur R. Miller (Burkert 1999, p. 49). Still in 1971, a first unsuccessful draft bill for data protection was tabled in the *Bundesta*g (Hondius 1975, p. 37). In 1973, the German Government presented its proposal to the Parliament, starting a long process of requests for amendments by both the *Bundestag* and the Federal Council (*Bundesrat*) (Riccardi 1983, p. 248).

In January 1977, Germany finally enacted its first Federal Data Protection Law, under the heading *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* (*Bundesdatenschutzgesetz*, BDSG),[21] or Act on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act). The Act complemented existing legislation at the State level by focusing on data processing in the private sector, not yet covered. The Act's stated purpose was to protect personal data against misuse during their storage, transmission, modification or deletion (thus, in general, during data processing operations) for the safeguarding of the interests worthy of protection of the persons concerned.[22] Some have interpreted this allusion to interests worthy of protection as referring to the right to privacy (Riccardi 1983, p. 248), but actually the BDSG itself does not mention expressly any directly equivalent notion. As a matter of fact, in line with the 1970 Hesse Data Protection Act, the 1977 Federal Data Protection Law was particularly elusive as to the interests or values it aimed to substantiate (Bygrave 2002, p. 8), and in any case failed to include overt references to any right to privacy, or to private life (Mayer-Schönberg 1997, p. 224).

The basic principle of the 1977 BDSG[23] is that the processing of personal data is forbidden, unless it falls under one of the two conditions explicitly mentioned: if authorised by the BDSG or another law, or if on the basis of the consent of the individual.[24] Thus, on the one hand the Act appears to embody a strict approach to the processing of personal data, by globally proscribing it, but, on the other hand, it also advances a wide and extremely elastic avenue to sidestep the general proscription, namely obtaining the consent of the person concerned by the data. This prominent role granted to consent was one of the major peculiarities of the BDSG.[25] Another

[19] Of the University of Regensburg.

[20] Whose text had been partially translated into German by IBM in 1970 (Burkert 1999, p. 49).

[21] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Law on protection against the misuse of personal data in data processing) (Bundesdatenschutzgesetz—BDSG) (Federal Data Protection Act) of 27 January 1977, Bundesgesetzblatt (BGBl) 1 S 201.

[22] 'Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken' (sec 1(1) BDSG 1977).

[23] As noted in Sect. 3, described as comprehending the Act's ratio legis (Riccardi 1983, p. 248).

[24] *'... wenn.... der Betroffene eingewilligt hat'* (sec 3 BDSG 1977). The German noun for 'consent' is *Einwilligung*.

[25] In this sense, see notably: (Kosta 2013, p. 50 and 383).

characteristic feature of the German Federal Law is that it is broadly applicable to 'personal data' (a category defined as details on personal or material circumstances of an identified or identifiable physical person) as a whole, without establishing any distinctions between ordinary and special (or more sensitive) personal data (Riccardi 1983, p. 249). In addition, the Act created a *Bundesbeauftragter für den Datenschutz* (or Federal Data Protection Commissioner),[26] and established the obligation to appoint an internal 'data protection officer' (*Beauftragter für den Datenschutz)* for some private parties.[27]

3.1.4 France

France, like Germany one of the founding members of the EC, adopted soon after its own ad-hoc data processing rules. In France, discussions on the advent of computerisation and the protection of the individual originated under another label, different from 'data protetcion': the notion of *informatique et libertés*. The term *informatique* had entered French language in 1962 (Rey 1998, p. 1833), and is commonly translated, in this context, as computers.[28] Through the lens of the defense of *libertés*, France was precisely around that time refining its own doctrine on the protection of individuals, encompassing the safeguarding of their *vie privée* or private life.[29]

French public authorities started to undertake studies on the relation between freedoms and computers at the end of the 1960s.[30] In 1970, a French deputy, Michel Poniatowski, submitted a legislative proposal[31] to the Assemblée Nationale for the creation of both a Commission monitoring the use of computers (*Comité de surveillance de l'informatique*)[32] and an ad-hoc Tribunal on computer-related issues (*Tribunal de l'informatique*). The proposal was unsuccessful. It was followed by other similar proposals, also unlucky.[33] In 1971, nevertheless, the *Conseil d'État*

[26] Section 17 of BDSG 1977.

[27] Section 38 of BDSG 1977.

[28] It can also mean computer science.

[29] See Chap. 2, Sect. 2.2.2.2, of this book.

[30] Jean Foyer, Rapport fait au nom de la Commission de lois constitutionnelles, de la législation et de l'administration générale de la République sur 1° le projet de loi (N° 2516) relatif à l'informatique et aux libertés; 2° la proposition de loi (n° 1004) de M. Cousté tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens; et 3° la proposition de loi (n° 3092) de M. Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique (1978) (see Section 'Les origines de projet de loi').

[31] Proposition de loi n° 1454 (proposition de loi Poniatowski), 30 Octobre 1970.

[32] According to the bill, owners of computer devices were to inform the commission of all details of their use of the information processed (Robert 1977, p. 287).

[33] Other proposals were advanced by the Président Laroque of the Conseil d'Etat and by the Syndicat national de la magistrature (Hondius 1975, p. 34).

decided to engage in studying the subject (Commission informatique et libertés 1975, p. 7).[34] And in 1972, at the Ministry of Justice, a working group named *Informatique et vie privée* was instructed to discuss the possible problems linked to a regulation of computers (Robert 1977, p. 290). Their common conclusions described a risk inherent to computer science, from which they inferred a need to legislate (Boucher 1980, p. 46).

In 1974, just as he was starting to explore these developments, a journalist writing for Le Monde learned about a project called S.A.F.A.R.I. (for *Système Automatisé pour les Fichiers administratifs et le Répertoire des Individus*) (Boucher 1980, p. 45), foreseeing the linkage of disparate information stored by different French public administrations through a unique identifier (About and Denis 2010, p. 96). In March 1974, the journalist published an article titled '*Safari ou la chasse aux Français*' ('SAFARI or the hunt of the French'), which caused great public alarm. Different reactions from the Government then in place came quickly, but only a few days later the President of the French Republic, Georges Pompidou, died, leading to a series of governmental changes that eventually saw Michel Poniatowski become Minister of Home Affairs. Poniatowski, now Minister, took the opportunity to launch again his personal idea of creating a special Commission for the monitoring of computers, as already advanced in 1970. In the meantime, additionally, a legislative proposal for the creation of a Control commission on data processing (*Commission de contrôle des moyens d'informatique*) to protect the *vie privée* and individual freedoms had been submitted to the Assemblée Nationale, by Pierre Bernard Cousté,[35] who alluded in the proposal's explanatory memorandum to the 1970 Data Protection Act of the federal state of Hesse and other related initiatives undertaken in European countries, and argued that, in the absence of common ground rules in this field at the level of the European Communities, France had to take action.[36]

Still in 1974, another body was established at the Ministry of Justice, now under the name of *Commission informatique et libertés* (Hondius 1975, p. 34),[37] with the mandate of recommending concrete future steps in the area.[38] Looking for guidance, this Commission analysed the state of discussions in international organisations such as the United Nations, UNESCO and the Council of Europe, but also, and with particular attention, at the Organisation for Economic Co-operation and Development (OECD) (Commission informatique et libertés 1975, p. 9).

The OECD, an international economic organisation of industrial countries founded in 1961, was conveniently headquartered in Paris, and had been working on the

[34] In 1969/1970, a yearly report to the Conseil d'Etat emphasised the need to interrogate the consequences of the development of computers on public freedoms and administrative decisions (Bertrand 1999, p. 123).

[35] Proposition de loi tendant à créer une Commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens, submitted on 4 April 1974**.**

[36] Ibid. 4.

[37] The Commission was chaired by Bernard Chenot, vice-president of the Conseil d'État.

[38] The First Minister of the time, Pierre Messmer, announced that any interconnection of files would be forbidden waiting for the results of the Commission's work (Armatte 2002, p. 16).

question of computers since the end of the 1960s. In June 1974, the OECD held a special event titled *OECD Seminar on Policy Issues in data protection and privacy*, which was attended by almost all the members of the French *Commission informatique et libertés*, and facilitated their awareness of the 1973 Swedish Data Act, and of the (still then to be adopted) US 1974 Privacy Act (Gassmann 2010, p. 2).

The *Commission informatique et libertés* decided to address the potentially broad issue of computers and freedoms without attempting to determine which freedoms were exactly impacted upon by the use of computers, arguing, instead, that freedom is indivisible (Commission informatique et libertés 1975, p. 89). Its conclusions, in the form of a report written by Bernard Tricot and Pierre Catala, were submitted to the French government in June 1975.[39] They included as series of reflections on the possible need to regulate the use of both 'nominal' and 'non-nominal' data, but stressed that the processing of 'nominal' data was particularly problematic, and that various countries granted as a principle the right to access for people to 'nominal data' about them (Commission informatique et libertés 1975, pp. 21–37). They also observed that the notion of 'sensitive data', understood as data related to the 'intimacy' of individual and family life, or racial, religious, political or similar information, was very relevant to understand the relation between computers and freedoms, even though it presumably only corresponded to a first approach to the problem (Commission informatique et libertés 1975, p. 47).

The report by the *Commission informatique et libertés*, generally known as the Tricot report, directly inspired a legislative proposal submitted to the Assemblée Nationale in August 1976. During the parliamentary debates on this proposal, communist deputy Lucien Villa alluded to a declaration on freedoms published in June 1975 by the French Communist Party,[40] according to which should be prohibited any secret collection of data about individuals, which also asserted the need to recognise a general right of access to nominal files, and furthermore solemnly announced that computers (*l'informatique*) must serve citizens.[41] Villa introduced an amendment to have this later idea inserted in the very first clause of the upcoming law. The Assemblée nationale acquiesced in the principle that the computer is to be regarded 'a servant',[42] and the amendment was approved.

The adopted *loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978* (Law on Computers, Files and Freedoms of 6 January 1978)[43] thus eminently establishes that computers must serve the citizen. Its Article 1 describes the Law's

[39] And made public in September 1975 (Foyer 1978, Sec. Les origines du projet de loi).

[40] Titled *Vivre libres!: projet de déclaration des libertés soumis à la discussion des Français*. Work on the drafting of that declaration had started in 1973, and one of its most active drafters had been Guy Braibant (Lemarquis 2013), who some years before had already been discussing the impact of computers on individual freedoms, as well as possible remedies based notably on a right of access to personal information, mentioning notably Westin's research (see, for instance: (Braibant 1971)).

[41] 'Informatique et libertés', *Journal officiel de la République française* (Débats parlementaires, Assemblée nationale, Constitution du 4 octobre 1958, 5e législature, Première session ordinaire de 1977–1978, compte rendu intégral—2e séance, 1ère séance du mardi 4 octobre 1977).

[42] As expressed by Jean Foyer during the debates.

[43] Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

purpose as ensuring that computers must not be a prejudice for human identity, nor human rights, for the *vie privée* (private life/privacy), or individual or public freedoms.[44] The mention of 'human identity' in this context supposedly transpired a concern generated by the possible usage in France of a single identification number: it was felt that such single identification number would go against a notion of 'human identity' envisioned as requiring that everybody is addressed the way they address themselves, as opposed to through a number (Cadoux 1998, p. 217).[45] The mention of the protection of *vie privée* as only one concern among many others was a deliberate choice of its drafters, as noted later by Louis Joinet, one of the authors of the text.[46] By that time, it had already been observed that one of the peculiarities of the French approach was that it did not circumscribe the purpose of regulating the processing of data related to individuals to the single objective of protecting privacy or private life.[47]

The 1978 Law applied to 'nominal information' or *informations nominatives*, described as data allowing the identification of the person concerned by them,[48] when processed by either public or private parties. Compared to previous laws regulating data processing, the French one signified an extension of the rights of the individual, which were given a more significant role to play (Mayer-Schönberg 1997, p. 226). The Law proscribed the collection of data in a fraudulent, unfair or illicit manner,[49] and granted a general right to refuse processing,[50] detailing also the content a right to receive some detailed information when data were collected, and a right to access[51] and rectify collected data.[52] Furthermore, it imposed that 'nominal information' should not be stored longer than initially foreseen,[53] and always kept under strict security conditions.[54] The automated processing of nominal data able to reveal, directly or indirectly, information about race, political, philosophical or religious opinions, or trade union membership, was generally proscribed—although exceptionally permitted if on the basis of the consent of the individual concerned,

[44] Article 1 of Loi informatique et libertés 1978: 'Elle (l'informatique) ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques'.

[45] The solidity of this argumentation is nevertheless weak, considering that even first names that could perhaps be regarded as the way in which people call themselves can be linked to State identification practices (on the birth of the French *prénom* as a State practice: (Coulmont 2011, p. 7 and 8).

[46] And secretary of the Tricot Commission (Gassmann 2010, p. 6).

[47] Joinet referred to input provided in 1974 by the Italian Stefano Rodotà to the OECD, where Rodotà arued that in this way, and contrary to countries relying excessively on the use of the word privacy, France did not exclude for consideration other important issues (Joinet 1975, p. 67).

[48] Article 4 of Loi informatique et libertés 1978.

[49] Article 25 of Loi informatique et libertés 1978.

[50] Ibid. Article 26.

[51] Ibid. Articles 34–40.

[52] Ibid. Article 27.

[53] Ibid. Article 28.

[54] Ibid. Article 29.

by associations specifically active in any of these areas (on its own members), or by special legal authorisation.[55] Innovatively, the Law regulated automated decision-making.[56]

The French law created a *Commission Nationale Informatique et Libertés* (CNIL),[57] which was granted broad monitoring and sanctioning powers (Prieto Gutiérrez 1998, p. 1043), and was the first administrative authority of this kind formally portrayed as independent.[58] The instrument set up a system of prior authorisation of data processing activities based on a combination of a requirement of legal basis, for some instances, and a procedure of notification to the CNIL, for others.[59] And, despite its several national specificities, the 1978 Law asserted that the development of computers must take place in the context of international cooperation.[60]

3.1.5 Other Pioneering Acts

The laws described were only the first of many others that soon began to spread across Europe. The 1970s still witnessed the appearance of special statutes in other European countries, such as Denmark, Norway and Luxembourg.

Denmark was the first Scandinavian country to accede to the EC, which it entered in 1973. Since the 1960s, it had been contemplating possible legal strategies to reinforce the protection of individuals in the light of technological advances of the time, initially considering a review of its criminal law rules (Commission on Human Rights of the United Nations Economic and Social Council 1970, p. 14). Denmark adopted special rules on the processing of personal data in 1978, with two parallel acts (Blume 1991, p. 1): the *Lov om private register*[61] (Private Registers Act) regulated data banks in the private sector, whereas the *Lov om offentlige myndhigeders register*[62] (Public Authorities Registers Act) governed data banks held by public authorities (Burkert 1979, p. 25).[63] They both applied generally to all data processed electronically, as long as they referred to identifiable natural or legal persons. Special protection was granted to sensitive data (Burkert 1979, pp. 26–27).

Norway, which was not (and still is not) an EC Member State,[64] also adopted ad-hoc legislation in 1978. The first initiative towards legislation in Norway had been

[55] Ibid. Article 31.

[56] Ibid. Article 2.

[57] Ibid. Article 6.

[58] Article 8 of the Loi informatique et libertés 1978.

[59] Ibid. Articles 14–19.

[60] Ibid. Article 1.

[61] Lov nr 293 af 8 juni 1978 om private registre mv.

[62] Lov nr 294 af 8 juni 1978 om offentlige myndigheders registre.

[63] They were both adopted on 8 June 1978, and entered into force in January 1979 (ibid).

[64] Accession to the European Community was refused by referendum in 1972; a referendum held in 1994 similarly rejected accession to the European Union.

taken during the spring of 1970, when the Norwegian Government's Council for Computers in the Government contracted a group of university researchers headed by professor Knut S. Selmer to look into the issue, amidst rather vague references to US debates and initiatives within the OECD (Bing 1991, p. 169). The act adopted in 1978 was named the Data Registers Act.

Luxembourg, founding member of the EC, passed in 1979 its Act concerning the Use of Nominal Data in Computer Processing: *Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques* (Burkert 1979, p. 72).

3.2 Early Constitutional Recognition

As these legislative developments unfolded, some European countries were choosing instead a different path to address the regulation of data processing: the setting up of constitutional provisions. A special case in this context is Austria, which enacted a law that, while being an ad-hoc statute, partially enjoys constitutional status. Portugal and Spain represent the two other early examples of inclusion among constitutional provisions of specific references to data processing. None of these three countries was an EC Member State in the 1970s; they all acceded at a later stage: Portugal and Spain in 1986, and Austria in 1995.

3.2.1 Portugal

Historically, the first European country to incorporate specific provisions on automated data processing in its fundamental law was Portugal, which adopted its current Constitution in 1976. The 1976 Portuguese Constitution stands out from a comparative law perspective due to its lengthiness, and to the degree of detail with which it describes the fundamental rights and freedoms it establishes (Pérez Ayala 2007, p. 75). Article 35 of the 1976 Portuguese Constitution, titled 'Use of data processing', consisted originally of three paragraphs:[65] first, it granted all citizens a right to information on the content of all data banks concerning them, and a right to access to, and rectification of, the data;[66] second, it prohibited the automated processing of data concerning 'a person's political convictions, religious beliefs or private life', except if the data were in non-identifiable form; and, third, it proscribed the use of national unique numbers for the interconnection of data.[67]

[65] Constitutional reviews have later altered the content of Article 35 of the Portuguese Constitution, leading to an extension of the protection granted (Dias Venâncio 2007, p. 244 ff.).

[66] Article 35(1) of 1976 Portuguese Constitution establishes that all citizens shall have the right to information on the contents of data banks concerning them, and on the use for which they are intended, as well as to require the said contents to be corrected and brought up to date.

[67] Article 35(3) of the 1976 Portuguese Constitution foresees that citizens shall not be given all-purpose national identification numbers.

Article 35 of the 1976 Portuguese Constitution was instrumental for the later worldwide profileration of constitutional recognition of access to personal data. It was indeed one of the major sources of inspiration for the drafters of the Brazilian Constitution of 1988, which addressed the issue of access through the notion of habeas data,[68] an expression today particularly popular in Latin America (and sometimes depicted as a response to the divergences between the US and the EU) (Gakh 2006, p. 783).

3.2.2 Austria

In 1978, Austria adopted a *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz, DSG)*,[69] or Federal Act on the Protection of Personal Data, which included a first section on the *Grundrecht auf Datenschutz* or 'fundamental right to data protection' enjoying constitutional force.[70] The Act, thus, advanced a right called 'right to data protection' as a constitutionally protected fundamental right. The Austrian 1978 Federal Act, nonetheless, did not present such right as autonomous or independent, but as intrinsically linked to the right to respect for private and family life (*Privat- und Familienlebens)*. In this sense, Article 1 of Sect. 1 of the Austrian 1978 Federal Act established that 'everyone is entitled to have personal data relating to him kept secret', but only insofar as they have an interest in that data deserving protection, particularly with regard to the respect for their private and family life.[71] In Austria, rights recognised as fundamental can only be restricted under the conditions established by the European Convention on Human Rights (ECHR), which has itself constitutional status (Electronic Privacy Information Center (EPIC) and Privacy International (PI) 2007, p. 249).

[68] Article 5, inc. LXXII, title II of Brazilian Constitution: 'conceder-se-á habeas data: (a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; (b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo'. Already in 1985 Guatamela had adopted a Constitution including a provision applying to public archives and registers, which granted individuals access to them, and the right to have data rectified and updated, although without mentioning the notion of habeas data.

[69] Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz—DSG) BGBl. Nr. 565/1978.

[70] In Austria, constitutional protection is granted to all individual rights contained in statutory regulations enjoying constitutional ranking (*Verfassungsrang)* (Prakke and Kortmann 2004, p. 67).

[71] The orignal text establishes: 'Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens hat'. Article 2 of Sect. 1 concerned permissible limitations; Article 3 of Sect. 1 regarded a right to information and to access to the data; Article 4 of Sect. 1, a right to have data rectified or deleted; Article 5 of Sect. 1, further limitations; and Article 6 of Sect. 1, the protection of legal persons.

3.2.3 Spain

In Spain, work on a modern Constitution started in 1977, and culminated in the adoption of the Constitution of 1978.[72] The first drafts of the constitutional text already included a provision on the obligation for the legislator to limit by law the use of *informática* (or 'computers')[73] (Pérez Luño 2010, p. 381),[74] partially inspired in Article 35 of the 1976 Portuguese Constitution. The provision appeared as a component (the last one) of an Article that was to generate much debate in literature about its exact conceptualisation (Ruiz Miguel 1992, p. 144), namely Article 18.

Article 18 of the Spanish Constitution has four parts: in its first paragraph, it enshrines a right to honour, *intimidad personal y familiar* (translatable as 'personal and familiar intimacy, or privacy') and the own image; in its second paragraph, the inviolability of the home; in its third paragraph, the secrecy of communications, and, in its fourth and last paragraph, a mandate to limit the use of computers. As a whole, Article 18 lacks a specific name (Pérez Luño 2010, p. 338). It is thus unclear whether all of its four components are elements of a wider (unnamed) notion or not. If they were four facets of a single, general fundamental right,[75] the question would be then how to refer to such general fundamental right: possibly as a right to *intimidad* (which is however a term which appears to concern primarily Article 18(1), and not the other paragraphs), or perhaps as a right to *vida privada* (Espín Templado 2004, p. 15) (an expression that is a calque from French *vie privée*, and was used in 1979 for the official Spanish translation of Article 8 of the ECHR),[76] or even, maybe, as *privacidad* (an Anglicism already used by the Spanish Constitutional Court in the 1980s) (Martínez Martínez 2004, p. 67).[77]

Adding to the uncertainty generated by the structure of Article 18 of the Constitution, the definitive text of Article 18(4) stipulates that law shall limit the use of computers to ensure citizen's honour and the *intimidad personal y familiar*, but gen-

[72] Which received parliamentary approval on 31 October 1978, and entered into force, after being submitted to a referendum, on 29 December 1978.

[73] The Spanish word *informática* was imported from France, mirroring the French *informatique* (Ordóñez Solís 2011, p. 27).

[74] The text, with minor stylistic changes, came to be Article 17 of the document known as *Informe de la Ponencia*, and was later debate inside the Comisión Contitucional del Congreso (Pérez Luño 2010, p. 381).

[75] Some consider, for instance, that the confidentiality of communications and the inviolability of the home are part of the right to *intimidad*, while others believe it constitutes a separate right (Ruiz Miguel 1992, p. 144).

[76] The ECHR was incorporated to the Spanish legal order on 26 September 1979 (Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente, BOE número 243 de 10/10/1979, pp. 23564–23570).

[77] As an attempt to disentangle the notions of *intimidad*, *privacidad* y *vida privada*, see: (Del Castillo Vázquez 2007, p. 89 and 224).

erally also the full exercise of their rights.[78] Therefore, in a sense this provision can be read as a manifestation of the right to *intimidad* in the specific area of computers, but at the same time it expressly goes beyond serving the only purpose of ensuring *intimidad*, because it explicitly targets the full exercise of all rights.

Divergent conceptualisations of Article 18 of the Spanish Constitution were manifest during the discussion of the Constitutional project. Some deputies had called for the deletion of the mandate to limit the use of computers,[79] based on the understanding that the general provision on the protection of *intimidad personal y familiar* already globally prevented all types of interferences with such right, and that it was inappropriate, and unnecessary, to make an explicit reference to a particular technique of interference (Pérez Luño 2010, p. 381) which would eventually be surpassed by other techniques.[80] Conversely, others emphasised that data processing could not only interfere with the *intimidad* of individuals, but that more generally it could place individuals in a position of inferiority or inequality in many different situations, such as when trying to associate with others, or when engaging in an economic activity.[81] As a compromise solution, it was successfully proposed[82] to combine a reference to the need to regulate computers use to protect citizen's honour and the *intimidad personal y familiar* with an allusion to the need protect also in general the exercise of any of their rights.

The final construction of Article 18 read as an ensemble, and the wording of Article 18(4) in particular, left many issues undecided, in particular regarding the possible reading of Article 18(4) as establishing an autonomous fundamental right (Gómez Navajas 2005, p. 111)—not fully encompassed by the rights to honour and *intimidad personal y familiar*, as well as the incognita of its *nomen iuris* (or how should that right be called) (Álvarez García 2010, p. 65). These questions were to remain undecided during more than two decades (Guerrero Picó 2006, p. 179), until the Spanish Constitutional Court settled the question.

The recognition of a mandate to limit the use of computers in Article 18(4) of the Spanish Constitution was in any case accompanied by a recognition, among the constitutional provisions on principles of government and public administration,

[78] Article 18(4) of 1978 Spanish Constitution: 'la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'.

[79] Amendment number 716 of Sancho Rof (Unión de Centro Democrático (UCD), and Amendment 779, also by UCD.

[80] See intervention of Sancho Rof in 'Sesión número 9 de la Comisión de Asuntos Constitucionales y Libertades Públicas, celebrada el viernes, 19 de mayo de 1978 (1978)', *Diario de Sesiones del Congreso de los Diputados*, 70, 2526.

[81] Ibid. It was also unsuccessfully suggested (by Gastón Sanz, representing the Grupo Mixto) to reformulate the provision replacing the mandate to regulate the use of computers with an obligation to regulate the processing of personal data (Pérez Luño 2010, p. 382).

[82] By Miquel Roca Junyent, in the name of Minoría Catalana (Amendment 117). This amendment was also supported by the representative of the Grupo Socialista de Cataluña, Martín Toval, and the representative of the Grupo Comunista, Jordi Solé Tura. Finally, the amendments of the Grupo Mixto and the UCD were retired, and the one presented by Minoría Catalana was approved by unanimity (Pérez Luño 2010, p. 382).

of a right for citizens to access public archives and registers, with the exception of those affecting the security and defense of the State, crime investigation, and the protection of the *intimidad* of individuals.[83]

3.3 Summary

Whereas by the mid-1970s the US had inscribed in positive law a clear linkage between the regulation of data processed by computers and a redefined notion of privacy, European countries addressed the regulation of data processing through different legal mechanisms. The substance of these early European norms is certainly to a large extent comparable to US (informational) privacy, which can justify their labelling as 'broadly analogous' to US privacy law (Bennett 1992, p. 14). However, despite the diffuse convergence between US and Europe, as well as between European countries, pioneering European provisions also put forward specific regulatory principles, in addition to their displayed 'terminological idiosyncrasies' (Bygrave 2004, p. 322).

The Hesse Data Protection Act introduced the term *Datenschutz* ('data protection'). It applied exclusively to data automatically processed in the public sector. It focused on establishing applicable rules (as obligations of those processing data), and foresaw also some rights for the person concerned by the data processing, such as the right to rectify registered data. Additionally, it established a *Datenschutzbeauftragter*, or Data Protection Commissioner, to supervise compliance with the law. The Swedish 1973 Data Act aimed to prevent undue invasions on the personal 'integrity' of the person whose data were registered in data banks. Applicable to data processing by both public and private parties, it was grounded on the existence of a Data Inspection Board actively involved in dealing with specific data processing practices. In 1977, the BDSG confirmed that Germany was to regulate separately processing by public authorities (under the responsibility of the federal states) and by the private sector (addressed at federal level), as well as its endorsement of the *Datenschutz* tag. It identified this label with the premise according to which processing personal data is generally forbidden, unless authorised by law, or on the basis of the person concerned. It reaffirmed the German support to the establishment of Data Protection Commissioner, and introduced the function of internal data protection officers. Whereas the Swedish *Datalag* was advanced as serving *integriteit*, German data protection was at that time not associated to any fundamental right in particular.

With its 1978 law, France showed evidence of a vision of the regulation of data processing as necessarily including not only supervision by an expressly independent authority, but also a detailed series of rights granted to the persons concerned, ranging from the right to object to data processing to the right to access and rectify data. It also put on the table the possibility to grant reinforced protection to some special categories of data, and the regulation of automated decision-making. The

[83] Article 105(b) of 1978 Spanish Constitution.

French *loi informatique et liberté* targeted the protection of the *vie privée* (privacy/private life) of individuals, but also human identity, human rights, and individual and public freedoms in general.

Some European countries soon formally acknowledged automated data processing as an issue deserving constitutional-level protection. If sometimes this led to the allusion in adopted statutes to existing rights and freedoms (as in France), in other cases it led to the integration into constitutional texts of provisions on automated data processing (i.e. Portugal, Spain). Austria was the first country to explicitly enshrine a constitutionally protected right to *Datenschutz*, or 'data protection'. It did not, however, present it as autonomous, but as serving the insurance of the private life of individuals.

The spread of norms regulating data processing entered a new phase by the beginning of 1980s, when international organisations started to adopt international instruments on the subject. They had been actively working on their elaboration already during the 1970s.

References

About, lsen, and Vincent Denis. 2010. *Histoire de l'identification des personnes*. Paris: Éditions La Découverte.

Álvarez García Francisco Javier. 2010. El acceso por parte de las fuerzas y cuerpos de seguridad del Estado a ficheros de datos personales. In *Protección de datos personales y proceso penal,* ed. Ernesto Pedraz Penalva, 53–87. Las Rozas: La Ley.

Armatte, Emilie. 2002. Informatique et Libertés: De Big Brother à Little Sisters? *Terminal* 88 (Automne-Hiver): 11–21.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.

Bertrand, André. 1999. *Droit à la vie privée et droit à l'image*. Paris: Litec.

Bing, Jon. 1991. Data protection in Norway. In *Nordic studies in information technology and law,* ed. Peter Blume, 24–78. Deventer: Kluwer.

Blume, Peter. 1991. Introduction. In *Nordic studies in information technology and law*, ed. Peter Blume, Deventer: Kluwer.

Boucher, Philippe. 1980. La situation en France. In *Informatique et vie privée,* eds. Françoise Collard, Alain Roy, Michel Collard, Claude Javeau, Philippe Boucher, and François Rigaux. Bruxelles: Editions Labor.

Braibant, Guy. 1971. La protection des droits individuels au regard du développement. *Revue internationale de droit comparé* 23 (4): 793–817.

Burkert, Herbert. 1979. Organisation et méthodes d'opération des autorités de protection des données. In *Étude sur la confidentialité et la sécurité des données*: *Rapport final à la Commission des Communautés européennes,* eds. Gesellschaft für Mathematik und Datenverarbeitung (GMD), Institut national de recherche en informatique et en automatique (INRIA), and National Computing Centre (NCC), Section 2.

Burkert, Herbert. 1999. Privacy/Data Protection: A German/European Perspective. In *Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass*., 43–69. http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf.

Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

Bygrave, Lee A. 2004. Privacy in a global context—A comparative overview. *Scandinavian Studies in Law* 47:319–348.

Cadoux, Louise. 1998. Identité, identification, identifiants. In *Privacy: Seminarie Egmontpaleis 26 & 27 Nov. 1998*, 215–226, Brussel: Minister van Buitenlandse Zaken.

Commission informatique et libertés. 1975. *Rapport de la Commission Informatique et Libertés*. Paris: La Documentation Française.

Commission on Human Rights of the United Nations Economic and Social Council. 1970. Human Rights and Scientific and Technological Developments: Report of the Secretary-General (Addendum 1). E/CN.4/102.

Coulmont, Baptiste. 2011. *Sociologie des prénoms*. Paris: Éditions La Découverte.

Dammann, Ulrich, Otto Mallmann, and Spiros Smitis, eds. 1977. *Data Protection Legislation: An International Documentation/Die Gesetzgebung Zum Datenschutz: Eine Internationale Dokumentation*. Frankfurt a. M.: Alfred Metzner Verlag.

Del Castillo Vázquez, Isabel-Cecilia. 2007. *Protección de datos: Cuestiones constitucionales y administrativas—El derecho a saber y la obligación de callar*. Cizur Menor: Aranzadi.

Dias Venâncio, Pedro. 2007. A previsão constitucional da utilização da informática. *Revista de Estudos Politécnicos* V (8): 243–264.

Electronic Privacy Information Center (EPIC), and Privacy International (PI). 2007. *Privacy & Human Rights 2006: An International Survey of Privacy Laws and Developments.* Washington, D.C. and London: EPIC / PI.

Espín Templado, Eduardo. 2004. Prólogo. In *Una aproximación crítica a la autodeterminación informativa*, ed. Ricard Martínez Martínez, 15–19. Madrid: Thomson Civitas.

Flaherty, David H. 1979. *Privacy and Government Data Banks: An International Perspective*. London: Mansell.

Foyer, Jean. 1978. Rapport fait au nom de la Commission de lois constitutionnelles, de la législation et de l'administration générale de la République sur 1° Le Projet de Loi (N° 2516) relatif à l'informatique et aux libertés; 2° La Proposition de Loi (n° 1004) de M. Cousté tendant à créer une Commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens; et 3° La Proposition de Loi (n° 3092) de M. Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique. N° 3125, Assemblée Nationale, Constitution du 4 octobre 1958, Cinquième législature, Première session ordinaire de 1977–1978.

Frosini, Vittorio. 1984. La Convenzione Europea sulla protezione dei dati. *Rivista di Diritto Europeo* 24 (1 (gennaio—marzo)): 3–18.

Gakh, Maxim. 2006. Argentina's protection of personal data: Initiation and response. *I/S—A Journal of Law and Policy for the Information Society* 2 (3): 781–801.

Gassmann, Hans Peter. 2010. 30 Years after: The Impact of the OECD Privacy Guidelines, Address to the OECD Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and Its Working Party on Information Security and Privacy (WPISP), 10 March 2010. www.oecd.org/sti/interneteconomy/44945922.doc.

Gómez Navajas, Justa. 2005. *La protección de los datos personales*. Cizur Menor: Aranzadi.

Guerrero Picó, María del Carmen. 2006. *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Cizur Menor: Thomson Civitas.

Hondius, Frits W. 1975. *Emerging Data Protection in Europe*. Amsterdam: North-Holland Publishing Company.

International Commission of Jurists (ICJ). 1972. The Protection of Privacy. *International Social Science Journal* XXIV (3): 414–602.

Joinet, Louis. 1975. Informatique et libertés: Approche du problème par les autorités gouvernementales. In *Computer en Privacy: Automatisering van Persoonsinformatie En Bescherming van de Persoonlijke Levensfeer*, eds. Freddy Colson, Roger Depré, and Peter J. Hustinx. Leuven: Acco.

Kosta, Eleni. 2013. *Consent in European Data Protection Law*. The Hague: Martinus Nijhoff.

Lemarquis, René. 2013. "Guy Braibant" *Le Maitron—Dictionnaire biographique du mouvement ouvrier français*. March 4. http://maitron-en-ligne.univ-paris1.fr/spip.php?article17767.

Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.

Mayer-Schönberg, Viktor. 1997. Generational development of data protection in Europe. In *Technology and Privacy: The New Landscape,* eds. Philip E. Agre and Marc Rotenberg, 219–241. Cambridge: MIT Press.

Öman, Sören. 2004. Implementing data protection in Law. *Scandinavian Studies in Law* 47:390–403.

Ordóñez Solís, David. 2011. *Privacidad y protección judicial de los datos personales*. Barcelona: Bosch.

Pérez Ayala, Andoni. 2007. Tres décadas de evolución constitucional en Portugal (1976–2006). *UNED: Revista de Derecho Político* 70:65–134.

Pérez Luño, Antonio Enrique. 2010. *Derechos Humanos, Estado de Derecho y Constitución.* 10th ed. Madrid: Tecnos.

Pirandello, Luigi. 1904. *Il Fu Mattia Pascal*. Roma: Newton Compton.

Pirandello, Luigi. 1923. *The Late Mattia Pascal*. New York: Dutton.

Prakke, Lucas, and Constantin Kortmann. 2004. *Constitutional Law of 15 Member States*. Deventer: Kluwer Legal Publishers.

Prieto Gutiérrez, Jesús María. 1998. La Directiva 95/46/CE como criterio unificador. *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* 23–26: 1091–1173.

Rey, Alain, ed. 1998. *Dictionnaire historique de la langue française*. Paris: Dictionnaires Le Robert-Sejer.

Riccardi, J. Lee. 1983. The German Federal Data Protection Act of 1977: Protecting the right to privacy? *Boston College International & Comparative Law Review* VI (1): 243–271.

Robert, Jacques. 1977. *Libertés publiques*. Paris: Montchrestien.

Ruiz Miguel, Carlos. 1992. *La configuración constitucional del derecho a la intimidad*. Madrid: Universidad Complutense de Madrid.

Simitis, Spiros. 2006. Einleitung: Geschichte—Ziele—Prinzipien. In *Bundesdatenschutzgesetz*, ed. Spiros Simitis, 61–153. Baden Baden: Nomos.

Simitis, Spiros. 2010. Privacy: An endless debate? *California Law Review* 98 (6): 1989–2007.

Söderlind, Åsa. 2009. Personlig integritet som informationspolitik: Debatt och diskussion i samband med tillkomsten av Datalag (1973:289). Institutionen Biblioteks- och informationsvetenskap/Bibliotekshögskolan, Högskolan i Borås och Göteborgs universitet.

Steele, Jonathan. 2002. Data protection: An opening door? The relationship between accessibility and privacy in Sweden in an EU perspective. *Liverpool Law Review* 24:19–39.

Van Hoof, D. C., D. Verbruggen, and C. H. Stoll, eds. 2001. *Elsevier's Legal Dictionary*. Amsterdam: Elsevier.

Von Beseler, Dora, and Barbara Wüstefeld, eds. 1986. *Law dictionary: English-German, Englisch-Deutsch*. 4th ed. Berlin: Walter de Gruyter.

Chapter 4
The Materialisation of Data Protection in International Instruments

But one thing is certain: data protection is a reality.

(Hondius 1978)

By the end of the 1970s, various international organisations began to work actively towards the elaboration of international instruments dealing with the processing of information on individuals. International cooperation brought together European and non-European countries, including the United States (US). It eventually led to the parallel and intertwined elaboration of two key international instruments: the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD), adopted in 1980, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter, 'Convention 108') of the Council of Europe, of 1981.

This initial institutionalised international cooperation resulted in the labelling of existing and upcoming European rules on the processing of data as concerned with 'data protection', and their progressive linkage with the word 'privacy'. The embroilment between these expressions was to expand from the adopted international instruments directly into various European national legal orders. It was also crucially transferred into European Union (EU) law, where it survived during several decades, and where it is arguably not (yet?) completely undone.

This chapter analyses how such 'data protection'/'privacy' connection was incorporated into the OECD Guidelines and Convention 108, to contribute to a deeper understanding of its implications for the shaping of EU personal data protection. It also examines the impact upon national legal instruments of the adoption of Convention 108, and the only partial integration of its terminology and approach in the case law of the European Court of Human Rights (ECtHR).

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_4,

4.1 The OECD and its Guidelines

The OECD is an international economic organisation established in 1961 to promote economic development and world trade. Initially composed of 18 European countries, together with the United States and Canada, it has nowadays 34 members, including countries of South America and the Asia-Pacific region. Its headquarters are in Paris, and its official languages are English and French. In 1980, the OECD adopted its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which constituted the first international statement of principles regulating the processing of data—a text agreed upon which agreed both by the US and European countries (Working Party for Information Security and Privacy (WPISP) 2011, p. 12).

4.1.1 From the Computer Utilisation Group to the Data Bank Panel

The OECD started investigating the issue of computers in 1968, when a Ministerial Meeting on Science of OECD Countries was devoted to the issue of *Gaps in Technology*.[1] A few months later, the OECD Committee on Science Policy promoted the launch of a Computer Utilisation Programme, and the setting up of a Computer Utilisation Group to study the subject more deeply (Hondius 1975, p. 57). This Computer Utilisation Group[2] carried out a series of studies on electronic data banks, computers, and telecommunications, leading it to the discussion of issues of privacy and data protection (Hondius 1975, p. 57). In 1971, illustrating the increasing interest of the OECD in the question of privacy, a report on *Digital information and the privacy problem* was published under the Series *OECD Informatics Studies*.[3]

In 1972, the OECD created a board named the Data Bank Panel,[4] directly concerned with reflecting on the regulation of the processing of information about individuals in automated databases. The Data Bank Panel organised in 1974 an *OECD Seminar on Policy Issues in data protection and privacy*,[5] where many of the discussions centred on the notion of privacy as described by Westin (Braibant 1999, p. 8). The event comprised a session titled *Rules for Transborder Data Flows*,[6]

[1] The 3rd Ministerial Meeting on Science of OECD Countries, celebrated in March 1968.

[2] Working in close liaison with the Information Policy Group, and under the supervision of the OECD Committee for Science Policy (Hondius 1975, p. 58).

[3] To which were annexed an English and a French translation of the Hessen Data Protection Act (Gassmann 2010, p. 1). Other studies published as Informatics Studies were *Computerised Data Banks in Public Administration*, and '*Policy Issues in Data Protection and Privacy*' (Working Party for Information Security and Privacy (WPISP) 2011, p. 9).

[4] Chaired by chaired by the Swedish P. Svenonius.

[5] See also Chap. 3, Sect. 3.1.4, of this book.

[6] As well as other sections named *The Personal Identifier and Privacy*, and *Right of Citizen Access to their File*. A Synthesis Report was prepared by the OECD Secretariat in 1976 (Working Party

heralding the identification of what soon became the major issue of concern for the OECD in relation to the regulation of data processing: transborder data flows (Gassmann 2010, p. 1).

The expression 'transborder data flows' referred to the possibility to legally transfer data from a determined country to another. The 1973 Swedish Data Act, based on the idea that, generally, any automated processing operation required previous authorisation by a Data Inspection Board, had established a requirement to obtain an explicit authorisation before exporting any data outside Sweden (Kuner 2011, p. 14). As the 1970s unfolded and national norms on data processing continued to spread, different European countries included in their own legislation disparate mechanisms to restrict the export of data, in the belief that, otherwise, those processing data might be tempted to escape national regulation by surreptitiously transferring data to countries with less stringent protection, so-called 'data havens': this was so in Austria[7] and France,[8] but also in Luxembourg, and in Denmark (Kirby 1980, p. 3).

One of the major objectives of the OECD being the promotion of the expansion of world trade, this organisation worried about the possibility that national provisions would create barriers to the free flow of information, and, in this way, impede growth (Working Party for Information Security and Privacy (WPISP) 2011, p. 10). Some considered that, under the surface of a discourse on the protection of the individual surrounding the national norms on data processing, what was really at stake were measures conflicting with free trade, or what was described as 'data protectionism' (Kirby 1980, p. 4). Transborder data flows were thus rapidly placed high on the agenda. In 1977, the OECD Data Bank Panel organised a new event, this time called *Symposium on Transborder Data Flows and the Protection of Privacy*. During the event, Louis Joinet, at the time President of the French *Commission nationale de l'informatique et des libertés* (CNIL), emphasised the economic value and national interest of transborder data flows (Working Party for Information Security and Privacy (WPISP) 2011, p. 10). The symposium led to the dismantlement of the Data Bank Panel, and the creation, instead, of a new Expert Group.

4.1.2 The OECD Guidelines

Set up at the beginning of 1978,[9] this new OECD Expert Group[10] was immediately entrusted with the task of drafting guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data for the OECD (Michael 1994, p. 34).[11]

for Information Security and Privacy (WPISP) 2011, p. 9).

[7] Österreichisches Datenschutzgesetz von 1978, p. 32, 34.

[8] Article 24 of Loi no. 78–17 relative à l'informatique, aux fichiers et aux libertés.

[9] By the Committee for Scientific and Technological Policy (Kirby 1980, p. 13).

[10] Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data.

[11] It has been argued that the initiative was originally advanced by the French government (Michael 1994, p. 32).

The Expert Group was chaired by Michael Kirby, Chairman of the Australian Law Reform Commission which was at that time preparing new federal laws on privacy protection for Australia (Kirby 2010a, p. 2).[12] Other Expert Group members included the German Spiros Simitis, who had previously contributed to the drafting of pioneering German data protection, and was the *Hessischer Landesbeauftragter für den Datenschutz* (Data Protection Commissioner of the German federal state of Hesse) since 1975 (Kirby 2010a, p. 7), and the Italian Stefano Rodotà.

Among the main common references for discussion inside this Expert Group were the writings by Westin and by one of his former research assistants, the Canadian David Flaherty, as well as existing institutional reports, such as the British 1972 Younger Report, the French 1975 Tricot report, and especially, the report *Personal Privacy in an Information Society* published in 1977 by the short-lived US Privacy Protection Study Commission (The Privacy Protection Study Commission 1977). The OECD Expert Group was instructed to carry out its activities in close co-operation and consultation with both the Council of Europe, already active in the field for some years, and the European Community (EC) (Kirby 1980, p. 14),[13] which was starting to express interest in the field.

The negotiations leading to the elaboration of the OECD Guidelines were rather laborious (Bennett and Raab 2003, p. 74), notably due to contrasting approaches on the question of international data flows. And although there was a consensus on the idea that individuals should generally have access to personal data held about them (Kirby 1980, p. 5), views also diverged on how this should be put into words. European members favoured language similar to two recommendations already adopted by the Council of Europe[14] while US representatives insisted—with success—on referring back to the 1977 report by the US Privacy Protection Study Commission as the main 'conceptual framework' to apply (Kirby 1980, p. 16). Whereas Council of Europe's instruments tied the adoption of measures solely to the protection of individuals,[15] the l977 US report delineated the vision of a need to strike a proper balance between competing values: on the one hand, individuals' interests on their personal privacy, and, on the other, the information needs of an information-dependent society.[16]

In January 1980, US President Jimmy Carter announced in his State of the Union Address that the adoption of the OECD guidelines was imminent. The OECD Council finally adopted its Recommendation concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[17] in September 1980.

---

[12] Peter Seipel assisted as consultant.

[13] The Expert Group worked in cooperation with representatives of the Commission of the European Communities (EC) (Kirby 2010a, p. 8). The key representative of the Council of Europe was F. W. Hondius (Kirby 2010a, p. 8).

[14] Council of Europe's Recommendations 73 (22) and 74 (29).

[15] European representatives emphasised that for them interferences with privacy from misuse of personal data were not a theoretical danger, but had historical precedents, for instance in relation with the Second World War (Kirby 2010b, p. 5).

[16] See: (The Privacy Protection Study Commission 1977, Chap. 1 "Introduction").

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980. Actually, 21 of the then 24 Members of the OECD voted in favour,

The OECD Guidelines target the protection of 'privacy', as expressed in their heading, but, more exactly, 'the protection of privacy and individual liberties'[18] in relation to personal data. The mention of 'individual liberties' in conjunction with privacy echoes the allusion to the same notion among the general purposes of the 1978 French *loi informatique et libertés.*[19] It also translates a tension between the disparate terminological choices existing among OECD countries. The Preface to the OECD Guidelines states that 'privacy protection laws'[20] have been introduced or are to be introduced in many OECD Member countries, including France, Germany, Sweden, Belgium, the Netherlands or Spain, with a view to prevent 'what are considered to be violations of fundamental human rights'[21] in relation to the use of personal data.[22] The Explanatory Memorandum accompanying the Guidelines nevertheless concedes that in continental Europe it is common practice to refer to 'privacy protection laws' not with such terms but rather as 'data laws', or even as 'data protection laws'.[23] It also hints at the different meanings attached to the word privacy, arguing that there has been in the previous years 'a tendency to broaden the traditional concept of privacy', leading to something that 'can perhaps more correctly be termed *privacy and individual liberties'*.[24][25]

Privacy is any case the word in the end privileged by the OECD Guidelines, which repeatedly refer to privacy protection, and to the protection of privacy. Despite the qualifications of the Explanatory Memorandum, in the Guidelines themselves there is no reference whatsoever to data protection. As a matter of fact, they designate any existing norms on the processing of data as privacy laws. This choice was fully consistent with the US perspective, which formally endorsed (informational) privacy while ignoring the 'data protection' tag (a notion still today commonly overlooked both by US law and doctrine),[26] but it represented a novelty from the European standpoint, as in Europe at the time no existing legal instrument portrayed itself as a privacy instrument as such.

Concerning their substance, the OECD Guidelines apply to any personal data 'which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties', regardless of whether they are processed in the public or in the private

---

while Australia, Canada and Ireland preferred to abstain, and to postpone the decision the join (Commission nationale de l'informatique et des libertés (CNIL) 1982, p. 158).

[18] First paragraph of the Recommendation.

[19] The official languages of the OECD are English and French. In French, the title of the OECD Guidelines is *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* and their objective is described as ensuring protection of '*la vie privée et les libertés individuelles*'.

[20] First paragraph of the Recommendation.

[21] Ibid.

[22] Ibid.

[23] See Explanatory Memorandum, paragraph 4.

[24] Emphasis added.

[25] Ibid. paragraph 2.

[26] Observing such resistance: (Arzt 2005, p. 193).

sector, and of whether they are processed automatically or manually.[27] Personal data are defined as 'any information relating to an identified or identifiable individual (data subject)'.[28] The processing of data of personal data in the signatory countries shall be subject to eight 'principles': the collection limitation principle,[29] the data quality principle,[30] the purpose specification principle,[31] the use limitation principle,[32] the security safeguards principle,[33] the openness principle,[34] the individual participation principle,[35] and the accountability principle.[36]

The protection of privacy and individual liberties is not, however, the only objective pursued by the OECD Guidelines. There is a key second goal, which is the sheltering of transborder flows of personal data by avoiding any disparities in national legislations that could hamper 'the free flow of personal data across frontiers'.[37] Four different principles are put forward to facilitate the free flow of personal data across borders, including a general invitation to refrain from restricting transborder flows of personal data,[38] and a suggestion to avoid developing, in the name of the protection of privacy and individual liberties, any laws that would create obstacles to such flows.[39]

After adopting the 1980 Guidelines, the OECD remained active in the area of the regulation of data processing. For instance, in a Declaration on Transborder Data Flows accepted on 11 April 1985, the OECD Minister Committee reiterated the guidelines, while simultaneously emphasising again the interest of the OECD in unobstructed information exchange.

During all its various activities in the field, the OECD has confirmed its initial approach of subsuming any rules on the processing of data under the privacy tag. In this sense, in 2007 it adopted a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, and, for the purposes of that Recommendation, any 'national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines' are to be referred as 'laws protecting privacy'.[40] US literature commonly follows this line of thinking, for instance describing 'data protection' as a phrase 'frequently used' in Europe 'to describe privacy protection' (Solove et al. 2006, p. 870). The OECD Guidelines were an extremely influential instrument globally, but were not legally

[27] Article 2 of the OECD Guidelines.

[28] Ibid. Article 1(b).

[29] Ibid. Article 7.

[30] Ibid. Article 8.

[31] Ibid. Article 9.

[32] Ibid. Article 10.

[33] Ibid. Article 11.

[34] Ibid. Article 12.

[35] Ibid. Article 13.

[36] Ibid. Article 14.

[37] Ibid.

[38] Ibid. Article 17.

[39] Ibid. Article 18.

[40] Point 1 of Annex to OECD *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007).

binding. As they were adopted, the Council of Europe was finalising the elaboration of a legally binding instrument, to become even more significant in Europe.

4.2 The Council of Europe and Convention 108

The Council of Europe is an international organisation set up in 1949 by ten European countries,[41] to develop throughout Europe common and democratic principles. It comprises now 47 members. It is based in Strasbourg, and has two official languages: English and French.[42]

4.2.1 Privacy as (Insufficiently) Protected by Article 8 of the ECHR

Already in 1949, the Council of Europe launched negotiations to draft and adopt its own catalogue of human rights, leading to the elaboration of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Signed on 4 November 1950, and entered into force on 3 September 1953, the EHCR soon became the most important European human rights instrument ever. It lists thirteen rights or freedoms that drew heavily upon the Universal Declaration of Human Rights of 1948, both in subject matter and terminologically (Blackburn 2001, p. 9).

Contrary to the Universal Declaration of Human Rights (UDHR), however, the ECHR does not mention privacy at all. Whereas Article 12 of the UDHR, establishes that '(n)o one shall be subjected to arbitrary interference with his *privacy*,[43] family, home or correspondence, nor to attacks upon his honour and reputation', the ECHR provision that is supposed to mirror it, namely Article 8(1) of the ECHR, foresees that '(e)veryone has the right to respect for his *private*[44] and family *life*,[45] his home and his correspondence'.[46] This formal peculiarity of the ECHR could presumably be explained by taking into account the influence of the French expression

[41] The Statute of the Council of Europe was adopted on 5 May 1949, and came into force on 3 August 1949. The initial signatories were Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden and the UK. They were soon joined by Germany, Greece, Iceland, and Turkey (1949/1950). Austria joined in 1956. Cyprus in 1961, Switzerland in 1963, Malta in 1965 (De Schutter 2010, p. 21).

[42] Article 12 of the Statute of the Council of Europe (London, 5 May 1949).

[43] Emphasis added.

[44] Emphasis added.

[45] Emphasis added.

[46] Article 8(2) of the ECHR adds: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

vie privée, which was the expression used in the French version, consistently with the French version of Article 12 of the UDHR.[47]

In reality, initial English draft versions of the EHCR did include the word privacy, but the term was replaced by the idiom 'private life' a few months before the definitive signing of this instrument. In the documents of the *travaux préparatoires* (preparatory works) of the ECHR the appearance of the expression private life (instead of privacy) in the English draft can be dated to August 1950. Although it was common practice to underline in each subsequent draft the changes proposed in relation to the previous draft, the sudden replacing of privacy with private life was not identified as a change, in the sense that it was not underlined.[48]

As a result of this (not even underscored) move, the English and French versions of Article 8 of the ECHR might be regarded as looking superficially rather similar: one establishes a right to respect for 'private life', and the other for *vie privée*. Nevertheless, while the French text maintains a formal consistency with Article 12 of the UDHR, the consistency is lost in the English version.

Insofar as the ECHR is concerned, the ultimate interpreter of its provisions is the ECtHR, based in Strasbourg. Over the decades, the Court has systematically avoided using the word privacy to refer to any right protected by Article 8 of the ECHR.[49] In reality, no Council of Europe institution appears to have used the word privacy in that sense (i.e., referring to the content of Article 8 of the ECHR) in the period going from the original drafting of the ECHR up until 1967.[50] During those years, the rare documented occurrences of the term took place only anecdotally, for instance in relation to some spatial privacy needed in Council of Europe premises to facilitate free discussions,[51] in the frame of criticism of the secrecy of certain governmental debates,[52] or regarding the isolation of houses as foreseen by a debated housing code.[53]

---

[47] Article 12 of the UDHR: 'Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation'.

[48] Draft Convention adopted by the Sub-Committee on Human Rights (7th August 1950) in (Registry of the Council of Europe 1967, p. 17).

[49] The word tends to appear only exceptionally and only in specific contexts, for each time that the ECtHR considers the possible relevance of the 'reasonable expectations of privacy' doctrine, which originated in the US (see, for instance, *Gillan and Quinton v the United Kingdom* [2010] RJD 2010, App. No. 4158/05, § 61). See also, in relation to 'a sense of privacy' of patients: *Z v Finland* [1997] RJD 1997-I, App. No. 22009/93, § 95.

[50] According to the information available on the electronic repository of the archives of the Council of Europe.

[51] In discussions regarding the possible need to ensure 'the maintenance of the privacy of certain parts of the Assembly premises, so that they would reserved exclusively to Representatives and to competent Assembly services' (Council of Europe's Consultative Assembly 1949, p. 1128).

[52] There are references to 'Governments enveloped in the privacy of diplomatic conference', as well as to 'the privacy in which the Committee's debates are conducted' (Council of Europe's Consultative Assembly 1950a, p. 1430, 1653). The word is also used in alluding to a suggestion by Winston Churchill for an international meeting to be 'held in an atmosphere of privacy and seclusion' (Council of Europe's Consultative Assembly 1953, p. 47).

[53] In describing a draft Housing Code said to contain provisions relating to distribution of space and 'maintenance of the privacy of the home' (Council of Europe's Consultative Assembly 1950b,

The situation started to change in 1967, when Article 8 of the ECHR was indeed characterised as establishing a right to privacy (as opposed to private life).[54] This usage of the word privacy to allude to the right to respect for private life of Article 8 of the ECHR emerged in the specific framework of debates over the impact of scientific and technological developments in the protection of human rights. In April 1967, more precisely, the Consultative Assembly of the Council of Europe referred to its Legal Committee two motions, one for a resolution on human rights and modern scientific and technological developments in general, and another more concretely expressing concern about the spread of technical devices facilitating eavesdropping and other ways of interfering with the right to privacy, which called for a study on how to regulate such devices (Commission on Human Rights of the United Nations Economic and Social Council 1970, p. 24).

In January 1968, the Council of Europe's Legal Committee responded to these two motions by submitting a report to its Parliamentary Assembly (Committee on Legal Affairs and Human Rights 1968). The report generally reviewed the dangers to individual's rights inherent in developments of the time, ranging from illegitimate use of official surveys to manipulation by electric shocks and drugs, and brainwashing.[55] Presenting the report to the Council of Europe's Parliamentary Assembly,[56] Mr. Czernetz, an Austrian representative, noted that the Legal Committee argued it was necessary to study 'the question whether Article 8 of the Convention on Human Rights as well as national legislation in the member States adequately protect the right to *privacy*[57] against violations which may be committed by the use of modern scientific and technical methods' (Council of Europe's Consultative Assembly 1968, p. 754). The terminological inclination of the members of the Legal Committee to use the word privacy in this context was presumably connected with their familiarity with the work of Alan F. Westin, cited twice by Czernetz during his speech (Council of Europe's Consultative Assembly 1968, pp. 751–752).

Following this intervention, the Parliamentary Assembly of the Council of Europe adopted an influential Recommendation addressed to the governments of its Member States: Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments.[58] Recommendation 509 (1968) proclaimed that 'modern scientific and technical methods'[59] were 'a threat to the rights and

p. 153, 209).

[54] In relation to Article 8 and Article 10(2) of the ECHR, it is alluded to 'the need for protection of the right to privacy', allegedly 'often not taken adequately into consideration by the Press' (Council of Europe's Consultative Assembly 1967, p. 15).

[55] But also eavesdropping, phone-tapping, surreptitious observation, subliminal advertising, propaganda and the use of mass media, and lie detectors (Commission on Human Rights of the United Nations Economic and Social Council 1970, p. 24).

[56] Presentation of 31 January 1968.

[57] Emphasis added.

[58] Council of Europe, Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting).

[59] Recommendation 509 (1968) paragraph 8(i).

freedoms of individuals and, in particular, to the right to *privacy*[60] which is protected by Article 8' of the ECHR,[61] and called for a study on the subject.[62] As a result, Council of Europe's Committee of Ministers included[63] this subject matter in the intergovernmental Programme of Work of the Council of Europe for 1968–1969,[64] and the Committee of Experts on Human Rights was set to work on it.

Somehow surprisingly, the Committee of Experts on Human Rights judged that all of the technological developments mentioned in Recommendation 509 (1968) were reasonably under control. But, the Committee pointed out, there was something that had not been mentioned in the Recommendation that was actually giving rise to serious problems, and required urgent action: the issue of computers (Hondius 1978, p. 2). The Committee of Experts on Human Rights regarded as particularly doubtful whether Article 8 of the ECHR offered any satisfactory safeguards in this area, particularly because, in its view, Article 8 of the ECHR was only applicable to interferences by public authorities, and not by private parties,[65] leaving the issue only partly uncovered.

By the beginning of the 1970s, thus, the Council of Europe had reframed its original interest in the problem of the protection of individuals in the face of technological developments by apprehending it as a (computers and) (informational) privacy problem, encapsulated by a need to, first and foremost, regulate the use of computers—very much echoing formally the framing of the issue in the US, therefore. And it had also set off the use of the word privacy to refer to the content of Article 8 of the ECHR.

4.2.2 Council of Europe's Recommendation 73 (22) and Recommendation 74 (29)

Following Recommendation 509 (1968), the Council of Europe continued to work on the protection for the citizen against intrusions on privacy by technical devices. A special Sub-Committee,[66] charged with studying the civil, criminal and constitutional issues related to the subject, suggested that the Council of Europe should

[60] Emphasis added.

[61] Ibid.

[62] Ibid. paragraph 8(ii).

[63] In April 1968, having considered Recommendation 509 (1968).

[64] Explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series, no. 108 of 28 January 1981, p. 2.

[65] Explanatory Report accompanying Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers of the Council of Europe on 26 September 1973 at the 224th meeting of the Ministers' Deputies, paragraph 2.

[66] Working under the supervision of the European Committee on Legal Cooperation and in consultation with the European Committee on Crime Problems, and chaired by Gerald Pratt (Hondius 1975, p. 66).

concentrate on investigating the issue of electronic data banks, temporarily leaving aside any other aspects of privacy (Hondius 1975, p. 66).

As a result of this focused effort, the Council of Europe's Committee of Ministers adopted in 1973 Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.[67] One of the major arguments grounding its adoption was that it was urgent to act in order to prevent the surfacing of divergences between upcoming national laws.[68] The 1973 Resolution's Explanatory Report noted that only very few Member States of the Council of Europe had already enacted legislation 'on *data privacy*',[69] but that, in addition to existing laws,[70] it was necessary to consider that there were important bills providing indications of possible solutions, among which was highlighted a 1972 Belgian bill.[71] The Explanatory Report also observed that the US 1970 Fair Credit Reporting Act equally provided an interesting model for discussion.[72]

Resolution 73 (22) took the form of a recommendation to Member States to take the steps necessary to give effect to ten principles applying to personal information stored in electronic data banks in the private sector. Elaborated in its Annex and further expounded in the Explanatory Report, these ten principles related to: quality of the information stored; the purpose of information; ways in which information is obtained; period during which data should be kept; authorised use of information; informing the person concerned; correction and erasing of information; measures to prevent abuses; access to information; and statistical data.

Resolution 73 (22) mentioned privacy in its very title, sustaining the idea that the regulation of automated data processing serves the protection of privacy, even if it failed to define or delimit the notion. It also alluded to the notion of 'intimate private life', stating that, generally, 'information relating to the intimate private life of persons' should not be recorded, and that in any case it should not be disseminated.[73] For the purposes of Resolution 73 (22), the terms 'information' and 'data' were used as interchangeable words, in an attempt to overcome that some European countries appeared to be focusing on the protection of 'data', while others referred to their object as 'information' (Hondius 1975, p. 85).[74]

Whereas Resolution 73 (22) covered data banks in the private sector, in 1974, the Council of Europe adopted a new Resolution which applied, this time, to the public

[67] Committee of Ministers of the Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

[68] Explanatory Report of Resolution (73) 22, paragraph 2.

[69] Emphasis added.

[70] Such as the 1970 Data Protection Act of the federal state of Hesse, and the Swedish 1973 *Datalag*.

[71] Explanatory Report of Resolution (73) 22, paragraph 8.

[72] Ibid.

[73] The French version refers to the protection of *vie privée* in the title, and to '*informations concernant l'intimité des personnes'* in para 1 of the Annex.

[74] See also: The Explanatory Memorandum of Resolution 74 (29) 12.

sector: Resolution 74 (29) on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.[75] Resolution 74 (29) likewise took the form of a recommendation to the governments of Member States to take the steps to give effect to the principles applying to personal information set out in an Annex.[76]

By the end of 1974, experts at the Council of Europe considered that the body of law created across Europe for the protection of individuals against computerised records had acquired a name of its own, and that such name was 'data protection' (Hondius 1978, p. 3).[77] This body of law was nevertheless portrayed as an element of 'privacy', a term sometimes linked to its understanding as 'information(al) privacy' (Hondius 1975, p. 4), but sometimes used to refer to the content of Article 8 of the ECHR.

4.2.3 Council of Europe's Convention 108

Having adopted Recommendation 73 (22) and Recommendation 74 (29), the Council of Europe decided to pursue its work by reviewing how they were implemented and, in general, the state of advancement of national legislation in the area. A comparative study carried out in 1975 by the Secretariat of the Council showed that all national data protection regimes in Europe shared fundamental principles related with the quality of information, obligations imposed on the record-keepers, the rights of the persons whose data are stored (the 'data subjects'), public supervision (generally by a special authority), and the existence of procedural rules and sanctions (Hondius 1978, pp. 4–5). Nonetheless, the study also highlighted the existence of disparities, and presented them as a potential problem justifying further action.

In 1976, a Committee of Experts on Data Protection was set up, and placed under the authority of the European Committee on Legal Co-operation (CDCJ).[78] Its objective was to prepare a Convention for the protection of privacy in relation to data processing, to be ready for 1980 (Hondius 1978, p. 8). The Committee of Experts

[75] Committee of Ministers of the Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

[76] These principles, although extremely similar to those of Recommendation 73 (22) (Kirby 1980, p. 10), were however formally presented in a slightly different fashion. The Explanatory Memorandum accompanying Resolution 74 (29) only mentions the existence of eight principles.

[77] Data protection had been described as the 'legal rules and instruments designed to protect the rights, freedoms and interests of individuals whose personal data are stored, processed and disseminated by computers against unlawful intrusions, and to protect the information stored against accidental or wilful unauthorised alteration, loss, destruction or disclosure' (Hondius 1975, p. 1). For Hondius, an especially unfortunate terminological choice was the repeated mention by English speakers of the words computers and computer science. He called English speakers to adopt the word *informatics* instead of computer science, and of *informatician* instead of computer scientist, imploring the acceptance of this words by English speakers as 'a sacrifice asked of them for the sake of international cooperation' (Hondius 1975, p. 56).

[78] Explanatory Report of Convention 108, paragraph I.

on Data Protection worked from November 1976 to May 1979,[79] and was renamed the Project Group on Data Protection (CJ-PD) during 1978.[80]

The first meeting of the Committee of Experts on Data Protection resulted in an exchange of letters with the OECD, agreeing on cooperation and mutual assistance (Michael 1994, p. 33). Since that very initial stage, there was a common view on the need for the future Convention drafted by the Council of Europe to respect the principle of free international flow of information as supported by the OECD, and to refrain from laying obstacles in the way of international trade and commerce (Hondius 1978, p. 8).

Following a proposal by one of Council of Europe's experts, Frits W. Hondius, it was decided to draft a Convention that could be ratified not only by European countries, but also by countries outside Europe. The instrument was thus not named European Convention, but simply Convention.[81] This search for openness was confirmed and sustained by the direct participation in the preparatory works of observers from the OECD, and from four of its non-European states (Australia, Canada, Japan and the US). Observers from the EC, concretely the EC Commission, also took part.[82]

As the Convention was being drafted, exchanges between the Council of Europe and EC institutions increased. In 1979, the Secretary General of the European Parliament sent a letter to the Secretary General of the Council of Europe to inform him of the European Parliament's interest in progress in the field, illustrated by an attached Resolution on the subject endorsed soon before by the European Parliament.[83] In February 1980, the Parliamentary Assembly of the Council of Europe adopted a Resolution[84] welcoming European Parliament's interest,[85] and inviting it 'to direct its attention to how action within the framework of the European Communities could most effectively strengthen the principles and provisions to be embodied in the convention on data protection of the Council of Europe',[86] as well as to call on national parliaments to press for the introduction of legislation on data protection.[87]

On the same day that it approved such Resolution encouraging further work by EC institutions, Council of Europe's Parliamentary Assembly also adopted a

[79] First under the chairmanship of Louis Joinet (France), and subsequently of R. A. Harrington (Explanatory Report of Convention 108, paragraph 17).

[80] A working party, composed of the experts from Austria, Belgium, France, Germany, Italy, Netherlands, Spain, Sweden, Switzerland and the UK, met several times between the plenary committee meetings (ibid.).

[81] Explanatory Report to Convention 108, paragraph 24.

[82] As well as from Finland, and of the Hague Conference on Private International Law (ibid. paragraph 15).

[83] Parliamentary Assembly of the Council of Europe, *Protection of the rights of the individual in the face of technical developments in data-processing*, Doc. 4377, 11.6.1979.

[84] Resolution 721 (1980) on data processing and the protection of human rights, Assembly debate on 1 February 1980 (27th Sitting), text adopted by the Assembly on 1 February 1980 (27th Sitting).

[85] Resolution 721 (1980) paragraph 6.

[86] Ibid. paragraph 10(a).

[87] ibid. paragraph 10(b).

Recommendation on the possible inclusion in the very text of the ECHR of a right to the protection of personal data. In January 1980, had indeed been submitted to the Parliamentary Assembly an Opinion on *Data processing and the protection of human rights* (Lewis 1980), where it was stressed that Portugal,[88] Spain,[89] Austria and the German federal state of North Rhine-Westphalia had incorporated 'data protection' into their respective constitutional texts. The Opinion was based on a Report that stated that 'the idea of privacy is very difficult to define', but argued that, nevertheless, 'it is possible to tell when and who it may be infringed by the computerised use of personal data' (Parliamentary Assembly of the Council of Europe 1980, p. 5).

In response to that Opinion, Council of Europe's General Assembly, through its Recommendation 890 (1980) on the protection of personal data,[90] commenting that some states had 'made the protection of personal data a constitutional right',[91] and declaring that others planned to do so, recommended its Committee of Ministers to consider 'as part of the extension of the rights in the (ECHR), the desirability of including (…) a provision on the protection of personal data, by amending Article 8 or 10, or by adding a new article'.[92] Council of Europe's Committee of Ministers transmitted this Recommendation for opinion to two different committees, the Steering Committee for Human Rights, and the European Committee for Legal Co-operation.

A final version of the Convention on data protection was published in April 1980 (Michael 1994, p. 33). The Convention, to be commonly known as Convention 108,[93] was adopted by the Committee of Ministers on 17 September 1980, and it was decided to open it for signature only during a Session of the Parliamentary Assembly (Commission nationale de l'informatique et des libertés (CNIL) 1982, p. 157). This happened on 28 January 1981, when seven states already signed it.[94]

Convention 108 identifies as its object to secure for all individuals in the territory of the countries Party to the Convention respect for their rights and fundamental freedoms, and in particular (in the French version, *notamment*) for their right to privacy, with regard to automatic of personal data relating to them,[95] which is advanced as corresponding to the substance of the notion of 'data protection'.[96] Convention 108 thus marks a key step in the norms on the processing of personal

[88] Portugal had become of Member of the Council of Europe in 1976.

[89] Spain had become of Member of the Council of Europe in 1977.

[90] Text adopted by the Assembly on 1 February 1980 (27th Sitting).

[91] Resolution 890 (1980) paragraph 2.

[92] Ibid. paragraph 3.

[93] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108.

[94] Austria, Denmark, France, Germany, Luxembourg, Switzerland and Turkey (ibid.). See also: Explanatory Report to Convention 108, paragraph 17.

[95] Article 1 of Convention 108.

[96] Ibid. The Explanatory Report to Convention 108 defines data protection as 'the legal protection of individuals with regard to automatic processing of personal information relating to them' (paragraph 1).

data, for at least three reasons: first, it inscribes in a legally binding international instrument the English idiom 'data protection' (in the French version, *protection des données*), moving it beyond its previously strictly German context; second, it formally links such data protection to the safeguarding of 'rights and fundamental freedoms' in general; and, third, it articulates a special linkage of data protection with a 'right to privacy'—to be understood as enshrined by Article 8 of the ECHR (mentioned in the Explanatory Memorandum), and thus as equivalent to the right to respect for private life. From its perspective, thus, it can be supported that there exists, for the purposes of Convention 108, something called 'data protection' which is implemented to preserve something designated as 'privacy' (Flaherty 1989, p. xiv).

Contrary to the OECD Guidelines, which openly pursue two conflicting objectives that they aim to reconcile ('privacy and the free flow of information', the latter overtly related to OECD's support of the free market),[97] Convention 108 has, formally, one single purpose: ensuring data protection.[98] Nevertheless, Convention 108 is also directly concerned with securing the free flow of data. In this sense, it devotes various provisions to 'Transborder data flows',[99] and prohibits in general any restriction to flows of personal data going to the territory of another Party taken 'for the sole purpose of the protection of privacy'.[100]

Convention 108's backing of the free flow of personal data is connected in a rather indeterminate way both to the notion of free market and to freedom of expression, concretely through a renaming of the established human rights principle of freedom of circulation of information (Lageot 2008, p. 338) in terms of 'free flow' (which was the terminology applied by the OECD to refer to the lifting of barriers to free trade). The preamble to Convention 108 identifies 'the free flow of information between peoples' as a fundamental value, linking it to 'the freedom of information across frontiers'.[101] The Explanatory Report to the text explicitly links the Convention's provisions on transborder data flows to 'the principle of free flow of information, regardless of frontiers, which is enshrined in Article 10' of the ECHR,[102] proclaiming that the 'free international flow of information' is of fundamental importance for individuals as well as for nations.[103] The same Explanatory Report also asserts that the preamble aims at underlining the Convention 'should not be interpreted as a means to erect non-tariff barriers to international trade'.[104] Despite not being formally as overtly directed towards ensuring the free flow of

[97] Described as fundamental and competing values in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[98] Article 1 of Convention 108.

[99] Chapter III of Convention 108.

[100] Article 12(2) of Convention 108; see also Articles 12(1) and 12(3).

[101] Article 10(1) of the ECHR establishes in its first sentences: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.

[102] Explanatory Report to Convention 108, paragraph 62.

[103] Ibid. paragraph 9.

[104] Ibid. paragraph 25.

data as the OECD Guidelines, Convention 108 has been portrayed as at least as equally concerned with such objective (Jacqué 1980, p. 779).

The scope of application of Convention 108 covers 'automated personal data files and automatic processing of personal data in the public and private sectors'.[105] Contrary to the OECD Guidelines, it thus focuses on the processing of data which is automated. Personal data are defined as 'any information relating to an identified or identifiable individual ('data subject')'.[106] In the French version, the notion of 'personal data' is referred to as '*données à caractère personnel*', or 'data of personal nature', a wording underlining the peculiarity of the meaning of 'personal' in this context. The provisions of a Chapter titled '*Basic principles for data protection*' (which do not include any further references to such idea of principles) address, notably, the notion of quality of data,[107] special categories of data,[108] data security,[109] and additional safeguards for the data subject (which are to generate subjective rights in domestic law).[110] The notion of quality of data is particularly important: it refers to the idea that personal data automatically processed must be processed 'fairly and lawfully',[111] 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes',[112] 'adequate, relevant and not excessive' in relation to such purposes;[113] 'accurate and, where necessary, kept up to date',[114] and preserved in a form allowing for identification of individuals only as long as it is necessary.[115] Under the 'additional safeguards for the data subject' heading are recognised the right to information on the existence of automated personal data files, and on the controller of the files;[116] the right to access data stored,[117] the right to obtain rectification or erasure of the data if unduly processed,[118] and the right to have a remedy in case of lack of compliance.[119]

Convention 108 created a Consultative Committee (T-DP), consisting of representatives of Parties to the Convention and complemented by observers, which was entrusted with the interpretation of its provisions, their insurance, and the

[105] Article 3(1) of Convention 108.

[106] Ibid. Article 2(a).

[107] Ibid. Article 5.

[108] Ibid. Article 6.

[109] Ibid. Article 7.

[110] Ibid. Article 8.

[111] Ibid. Article 5(a).

[112] Ibid. Article 5(b).

[113] Ibid. Article 5(c).

[114] Ibid. Article 5(d).

[115] Ibid. Article 5(e).

[116] Ibid. Article 8(a).

[117] More concretely, 'to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form' (Article 8(b) of Convention 108).

[118] Ibid. Article 8(c).

[119] Ibid. Article 8(d).

improvement of their application.[120] Decades later this T-DP was merged with the Project Group on Data Protection set up in 1978.[121]

One of the first effects of the adoption of Convention 108 was to put over the possible inclusion in the ECHR of a special provision on data protection. The two committees to which the Committee of Ministers had transmitted Recommendation 890 for opinion, namely the Steering Committee for Human Rights, and the European Committee for Legal Co-operation, agreed shortly after the Convention's approval that it was not appropriate at the time to draft a provision on the protection of personal data for incorporation in the ECHR (Committee of Ministers of the Council of Europe 1981, p. 27). They suggested that it was preferable to first acquire more experience on the application of Convention 108, while at the same time working towards sector-specific Recommendations complementing it (Committee of Ministers of the Council of Europe 1981, pp. 28–29). The Steering Committee for Human Rights also pointed out the importance of the case law of the ECtHR confirming that States had positive obligations in relation to Article 8 of the ECHR,[122] asking to consider the possible implications of such case law as regards the provision of sufficient safeguards against interference with privacy resulting from the use of automatic processing of personal data—an argument that, in reality, could have been used to question also the need to adopt Convention 108.

Convention 108 entered into force on 1 October 1985, obliging participating countries to adopt their own legislation. It immediately generated much interest in the EC Commission, which did not only promote the Convention's ratification by Member States, but also expressed its intention to accede to the instrument. In 1999, Convention 108 was amended to allow the accession of the European Communities.[123] In 2001, an Additional Protocol was open to signature, with supplementary provisions on supervisory authorities and on transborder data flows.[124] The Additional Protocol took Convention 108 closer to the EC regime, which was already developed by then: it had put on the table the requirement of an independent data protection authority as a key element of data protection enforcement, and had refined the approach to requirements for restrictions on personal data exports.

The 1981 Convention is currently under reconsideration. The review process, conducted by the T-PD, started formally in January 2011 (Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to

[120] Chapter V of Convention 108.

[121] The merge occurred in 2003, and the resulting committee kept the name of Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

[122] It referred notably to *Marckx v Belgium* [1979] Series A No. 31, App. No. 6833/74 (Committee of Ministers of the Council of Europe 1981, p. 27).

[123] Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, 15.6.1999.

[124] Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows, Strasbourg, 8.11.2001. See, notably: (Pavón Pérez 2002).

Automatic Processing of Personal Data (T-PD) 2011, p. 5).[125] In its context, the possibility is being discussed to include in the revised instrument an explicit reference to a 'right to data protection', more recently advanced as a right to the protection of personal data.

Concretely, it has been proposed that the future instrument should mention in its preamble that everybody has 'the right to control one's own data and the use made of them', and that the future Convention's opening provision should define its purpose as to secure for every individual 'the right to the protection of personal data, thus ensuring the respect for their rights and fundamental freedoms, and in particular their right to privacy, with regard to the processing of their personal data' (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 9). To justify the allusion to the right to the protection of personal data, it has been argued that the right 'has acquired an autonomous meaning over the last 30 years', both through the case law of the ECtHR, and in the Charter of Fundamental Rights of the EU (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 32).

Some Members of the Council of Europe, however, have manifested their reticence. German representatives have contended that the German government 'finds it difficult to draw the line between the 'right to data protection' and the 'right to privacy'' because '(i)n the German understanding, the right to data protection is derived from the right to privacy'.[126] And the Swedish delegation to the T-PD has expressed its uneasiness with the aforementioned sentence on the right of individuals to control their own data, observing that 'it is unclear what it means',[127] and it also advocated that any reference to 'data protection' shall be replaced with 'personal data protection' (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 107).

4.2.4 Impact of Convention 108 on National Laws

The adoption in 1981 of Convention 108 set a milestone in the development of norms on the processing of personal data in European countries.[128] This does not

[125] Works towards the review at started at T-PD level in 2009 (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 4).

[126] Comments of the German Federal Government regarding the planned overhaul of Council of Europe Convention 108 (30 May 2012) in (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 86).

[127] See (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 107); in a similar vein, the European Data Protection Supervisor (EDPS) warned that 'there is not, literally speaking, a right to control one's data in the text' (of Convention 108) (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 135).

[128] According to the chronology by Spiros Simitis, it marked the beginning of a second phase in the development of data protection: (Simitis 2006).

mean that it was the sole reference for (or the sole reason behind) national norms approved after 1981. Nonetheless, its principles certainly served as basis for all subsequent European legislation (Zerdick 1995, p. 81), and inspired the review of instruments already in force (Prieto Gutiérrez 1998, p. 1140). Its ratification was openly supported by the EC,[129] and was eventually configured by a prior condition to access some instruments emerging in the context of increased European integration. Nowadays, all EU Member States have ratified Convention 108. The instrument is what is technically described as non self-executing, in the sense that it imposes on those countries wishing to ratify it the integration in their own legal systems of measures in compliance with its content.

The 1981 Convention appears to have been the decisive factor conducting the United Kingdom (UK) to finally adopt an Act on the automated processing of data (Prieto Gutiérrez 1998, p. 1145), in 1984.[130] It was entitled the Data Protection Act 1984, a name that already illustrates the influence of Council of Europe's framing of the issue (in terms of 'data protection' as opposed to 'privacy'). The Act's provisions do not mention any right to privacy (Flaherty 1989, p. 377), the existence of which was still a contested issue in British law, even if this absence was not an obstacle for some to assert that, for the purposes of the Act, data protection was essentially another name for privacy.[131] Like Convention 108, the Data Protection Act of 1984 focused on the regulation of automated data processing. Its basic approach was to require public and private organisations with access to computer-held personal data to register with a Data Protection Registrar. Very much influenced by both Convention 108[132] and the UK Data Protection Act of 1984, Ireland passed in 1988 its own Data Protection Act.[133]

In 1987, Finland, the last Nordic country to enact a statute on the processing of data (Blume 1991, p. 1), finally adopted its Personal Data File Act,[134] which came into force in 1988.[135]

In the Netherlands, the Koopmans Commission, which had been reflecting on the issue of privacy and personal information since 1971,[136] published its final findings in 1976. On this basis, in 1981 a bill was put forward, but it was later withdrawn due to criticism on potential implementation problems. In 1985, a new bill was submitted, this time taking into account a major revision of the Dutch Constitution that had taken place in 1983, and which had incorporated in the constitutional text a general right to respect of the *persoonlijke levenssfeer* ('personal sphere of

[129] Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31.

[130] The UK signed Convention 108 in 1981, and ratified it in 1987.

[131] For instance: (Sizer and Newman 1984, p. 9).

[132] Ireland signed Convention 108 in 1986, and ratified it in 1990.

[133] Adopted on 13 July 1988, it came into force on 19 April 1989.

[134] Act 471/1987.

[135] Finland only signed and ratified Convention 108 in 1991.

[136] See Chap. 2, Sect. 2.2.1, of this book.

life')[137] together with a mandate to protect this right in relation to the recording and dissemination of personal data,[138] and on the rights to access to and rectification of such data.[139] The 1985 bill was enacted in 1989 as the *Wet persoonsregistraties* (WPR) (Overkleeft-Verburg 1995, p. 571).

Belgium signed Convention 108 already in 1982, but ratified it only in 1993. During many years it witnessed the drafting of unsuccessful bills (Robben and Dumortier 1992, p. 59), initially focusing on the regulation of the protection of private life in general,[140] later moving to certain aspects of such private life,[141] and later still centred on the protection of private life in relation to the processing of personal data.[142] In 1992, Belgium enacted the *Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.*[143]

4.3 European Court of Human Rights Case Law

As described, at the beginning of the 1970s, in order to justify Council of Europe's activity in the field of automated data processing that eventually resulted in the adoption of Convention 108,[144] it had been argued that Article 8 of the ECHR did not offer enough protection for individuals in the light of the advent of computers. A decade later, it was conversely contended that the very same Article, as developed in the case law of the judiciary of the Council of Europe,[145] was possibly effective enough to offer satisfactory protection, and that it was thus unnecessary to incorporate into the ECHR the recognition of an additional right.[146] In reality, both propositions might be regarded as open to debate.

The Council of Europe's Court that hears applications of alleged breaches of rights enshrined in the ECHR is the ECtHR. Over the decades, the ECtHR has been developing a broad interpretation of Article 8 of the ECHR. This interpretation certainly covers at least partially the scope of application falling under Convention 108, although it is still debatable whether it encompasses, or can encompass, the entirety of such scope (European Union Network of Independent Experts in

[137] Article 10(1) of the Dutch Constitution.

[138] Ibid. Article 10(2).

[139] Ibid. Article 10(3).

[140] Period 1970–1971 (Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.) 2004, p. 4).

[141] Period 1975–1976 (Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.) 2004, p. 4).

[142] 'Gol project', 1984–1985 (Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.) 2004, p. 4). See also: (De Hert and Gutwirth 2013, pp. 19–20).

[143] 08/12/1992 (B.S., 18.03.1993). Describing it as largely inspired by French law: (Reidenberg and Schwartz 1998, p. 12).

[144] See Sect. 2.1 of this chapter.

[145] The European Commission and the Court of Human Rights, which were dissolved with the coming into force in November 1998 of Protocol No. 11 to the ECHR.

[146] See Sect. 2.3 of this chapter.

Fundamental Rights 2006, p. 90)—and to what extent it grants, or can grant, an equivalent level of protection.

Article 8 of the ECHR, titled 'Right to respect for private and family life', has a binary structure. It reads as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In its first paragraph, Article 8 of the ECHR establishes the existence of a series of rights: a right to respect for private life, a right to family life, a right to inviolability of the home, and a right to confidentiality of correspondence. The ECtHR however often mentions these rights in conjunction with each other, for instance by referring jointly to the right to respect for private and family life, or to respect for private life and confidentiality of correspondence in combination (Nardell 2010, p. 46). The second paragraph of Article 8 of the ECHR details the requirements of lawful interferences by public authorities with the described rights, which need to be 'in accordance with law' and 'necessary in a democratic society', and to pursue one of the explicitly enumerated aims.

When adjudicating on Article 8 of the ECHR, the ECtHR typically follows a two-step approach: first, it examines whether the issue at stake shall be regarded as an interference with any of the rights mentioned; second, it appraises whether the interference is to be considered legitimate or not.[147]

4.3.1 A Broad Interpretation of the Right to Respect for Private Life

The ECtHR has given to the wording of Article 8(1) of the ECHR a wide, generous interpretation (Nardell 2010, p. 46), as an element of its general approach of regarding the ECHR as a living instrument to be interpreted each time in light of 'present-day conditions'.[148] This broad reading has allowed the Strasbourg Court to consider as interferences with the rights enshrined by the provision measures related to the processing of data about individuals, and, vice versa, adjudication on this kind of measures has contributed to the progressive extension of ECtHR's construal of Article 8 of the ECHR.

The Court's broad conception of private life was notably put forward in the *Niemietz* ruling.[149] In this judgment, the ECtHR stressed that the right to respect for

[147] As a landmark case, see: *Klass and others v Germany* [1978] Series A no. 28, App. No. 5029/71.

[148] *Tyrer v United Kingdom* [1978] Series A No. 26, App. No. 5856/72.

[149] *Niemietz v Germany* [1992] Series A No. 251-B, App. No 13710/88.

private life ex Article 8 of the ECHR includes to a certain degree the right for individuals to develop relationships with other human beings.[150] The Court declared that it regarded as both impossible and unnecessary to attempt to define the notion of private life, but that in any case it would be too restrictive to limit the notion to an 'inner cycle' in which the individual may live his own personal life as he chooses', excluding entirely the outside world. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings'.[151]

The *Niemietz* case concerned the search of a lawyer's office in the context of criminal proceedings against a third party, raising the issue of the protection granted to profession or business activities. During the search, various cabinets and files had been examined, but no relevant documents had been found. In its judgment, the ECtHR made it clear that there was no reason of principle why the notion of private life should be taken to exclude professional or business activities, since it is precisely in the course of their working lives that the majority of people have a significant opportunity of develop relationships with others.[152] In addition, the Court noted, in some cases it is not even possible to clearly distinguish which activities are part of a professional or business life, and which are not.[153] The ECtHR has since then regularly emphasised the wideness of the notion of private life, portraying it as a term 'not susceptible to exhaustive definition'.[154]

4.3.2 Protection of Information Relating to Private Life

The cornerstone of the Strasbourg's case law on the processing of information about individuals is possibly the 1987 *Leander* judgment.[155] Previously, the question of whether the Court should rely or not on the provisions of Convention 108 had already been touched upon in the *Malone* judgment of 1984, in relation to the monitoring of telephone communications by the police, within the context of criminal investigations, through a technique called 'metering', and the related storage of information.[156] In *Malone* the Court concluded that there had been a violation of

[150] *Niemietz* § 29. See also: (Sudre 2005, p. 402). This broad conception was partly based in a special use of the expression 'right to respect for private and family life' as referring to a nebulous notion that covers the right to develop interpersonal relations (Sudre 2005, pp. 403–404).

[151] *Niemietz* § 29.

[152] Ibid.

[153] Ibid.

[154] *Bensaid v United Kingdom* [2001] RJD 2001-I, App. No. 44599/98, § 47.

[155] *Leander v Sweden* [1987] Series A No. 116, App. No. 9248/81. See also: (Peers 2006, p. 507).

[156] *Malone v the United Kingdom* [1984] Series A No. 82, App. No. 8691/79. Concerning 'metering', the Court took note of the fact that a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, and that metering is therefore to be distinguished from interception of communications. The Court did not accept, however, that the use of data obtained from metering cannot give rise to an issue under Article 8 of the ECHR, as the records of metering contain information which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of

Article 8 of the ECHR in connection with these practices, but without explicitly referring to Convention 108. The judgment was however accompanied by the concurring opinion, signed by Judge Pettiti, in whose view it was impossible to isolate the issue of the interception of communications from the issue of data banks, because interceptions give rise to storing of the information obtained; in this context, Judge Pettiti referred to the principles established by Convention 108 as criteria relevant to assess whether or not a measure constitutes a violation of Article 8 of the ECHR.

In *Leander*, the ECtHR did not refer either to Convention 108 (Martínez Martínez 2004, p. 196), but declared that the mere storing by the police of information relating to the private life of an individual amounts to an interference with the right to respect for private life,[157] and that this is so independently of the possible subsequent use of the data in question.[158] The case concerned a Swedish carpenter who wished to work at a museum adjacent to a restricted military security, but, after a personnel control procedure, and seemingly on the basis of a secret police file, was refused the job.

The *Leander* judgment was important insofar as it advanced that the mere storage by the police of some information relating to the private life of individuals amounts to an interference with the rights established under Article 8 of the ECHR. The Court, however, critically failed to explain in what was grounded such qualification of data as relating to somebody's private life. In *Leander*, the ECtHR merely declared that it was uncontested that the data at stake in the particular case related to the private life of the individual,[159] which was true, because precisely one of the concerns raised by the applicant was that he had not been able to access the content of the secret file (De Schutter 2001, p. 153),[160] and this impossibility to access the data prevented any contestation regarding their nature.

Leander opened up the question of whether the category of 'information relating to private life' the mere storage of which can amount to an interference with Article 8 of the ECHR corresponded or not to the category of 'personal data' recognised in Convention 108, which covers any automated processing of personal data, including their storage. Convention 108 applies to personal data qualified as pertaining to 'special categor(ies)' of data, such as personal data 'revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life', or relating to criminal convictions,[161] but also, generally, to data not falling under any of such categories, which are nonetheless 'personal' data, defined as any information relating to an identified or identifiable individual.[162]

What appeared to generate major ambiguities, especially at the beginning, was the issue of whether in the expression information 'relating to the private life' of

---

the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 of the ECHR (§ 84).

[157] *Leander* § 48.

[158] In *Leander,* the ECtHR was additionally concerned with the release of information.

[159] *Leander* § 48.

[160] See also: (De Hert 1998, p. 1998).

[161] Article 6 of Convention 108.

[162] Ibid. Article 2(a).

individuals the adjective private shall be read as opposed to public, or not. In 1994, the Commission of Human Rights looked into the case of an Austrian citizen who had participated in a demonstration to draw attention to the plight of the homeless, *Friedl*.[163] The police had taken pictures of him, and stored them. The Commission of Human Rights, noting that there had been no intrusion of the 'inner circle' of the applicant's private life in the sense that he was not at home when the pictures where taken; that the photographs related to a public event, that he was attending freely; that they were taken to record the sanitary conditions of the demonstration;[164] that no names were noted on the pictures, with participants remaining unidentified, and that no personal data or images had been entered into a data processing system,[165] concluded that the measure did not amount to an interference with Article 8 of the ECHR.[166] The Commission did not assert, however, that any of these criteria excluded by itself the possible qualification of the measure as an interference with the right to respect for private life.

In 2000, the ECtHR put forward that the category of information 'relating to private life' (the storage of which can amount to an interference with the right protected by Article 8 of the ECHR) shall be understood in line with its broad reading of the notion of private life, which, it argued, corresponded also to the view sustained by Convention 108. In *Amann*,[167] the Court indeed recalled the principle established in *Niemietz* according to which there is no reason of principle to justify excluding activities of a professional or business nature from the notion of private life,[168] and maintained that this broad interpretation corresponds with that of Convention 108.[169]

The *Amann* case concerned a seller of depilatory appliances, who once received a telephone call from the Soviet embassy in Berne for the order of a machine called Perma Tweez. The call was intercepted by the public prosecutor's office, who requested the intelligence service to draw up a file about the seller. Recalling its *Leander* case law, and after connecting it to *Niemietz* and Convention 108, the Court concluded in the judgment that storing a card on the seller, on which he was described as 'a contact with the Russian embassy', and where it was pointed out that he did 'business of various kinds' with a certain company,[170] was to be regarded as containing details that 'undeniably' amounted to data relating to the applicant's private life.[171]

The matter was further developed in another judgment of the same year, *Rotaru,*[172] where the defendant tried to argue that Article 8 of the ECHR was not

[163] Commission (Plenary) *Friedl v Austria* [1994] RJD 31.

[164] Ibid. § 49.

[165] Ibid. § 50.

[166] Ibid. 51.

[167] *Amann v Switzerland* [2000] RJD 2000-II, App. No. 27798/95.

[168] *Niemietz* § 29, and *Halford v United Kingdom* [1997] RJD 1997-III, App. No. 20605/92, § 42).

[169] Amann § 65.

[170] Ibid. § 66.

[171] Ibid. § 67.

[172] *Rotaru v. Romania* [2000] RJD 2000-V, App. No. 28341/95.

applicable to the case on the grounds that the information stored related not to the applicant's private life, but to his public life.[173] In *Rotaru*, the applicant was a Romanian national complaining about information seemingly in possession of the Romanian Intelligence Service, and which he considered false and defamatory. The information had been revealed in a letter, and generally concerned his youth, covering also his political activities. The intelligence service had notably claimed he had participated to an extreme right-wing movement in the 1930s, apparently mistaking him with another individual of the same name.

In its judgment in *Rotaru*, the Court referred to *Leander* and *Amann,* and explicitly pointed out that 'public information' can also fall with the scope of 'private life', concretely when systematically collected and stored in files held by the authorities, and that this 'is all the truer where such information concerns a person's distant past'.[174] The ECtHR then noted that the letter in question 'contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than 50 years earlier',[175] and declared that 'such information, when systematically collected and stored in a file held by agents of the State', fell within the scope of private life for the purposes of Article 8 of the ECHR. *Rotaru* thus made clear that the category of information relating to private life shall not be read as opposed to public information. As this was clarified, the question remained of determining what is exactly information relating to private life, the mere storage of which can deserve qualification as an interference with the rights established by Article 8 of the ECHR.

Since then, the ECtHR has been throwing further light on the issue, often making use of criteria implicitly or explicitly associated to Convention 108.[176] In *P.G. and J.H.*,[177] for instance, the Court alluded to Convention 108 to develop the case law of *Rotaru* and to apply it to the recording of the applicants' voices when being charged and when in their police cell, commenting that '(p)rivate-life considerations may arise (…) once any systematic or permanent record comes into existence of (…) material from the public domain'.[178]

The 2008 *S and Marper* judgment[179] illustrates particularly well the variety of grounds that can justify the qualification of information as relating to private life for the purposes of considering that its mere storage amounts to an interference with

[173] Ibid. § 42.

[174] Ibid. § 43. See also: *Cemalettín Canli v Turkey* [2008] App. No. 22427/04, § 33. The case concerned a man who appeared in registers held by the police as former member of illegal organisations, despite having been acquitted of that offence.

[175] Ibid. § 44.

[176] The ECtHR generally takes into account the context and the way in which information is used, and its nature. See also, for example: *Peck v the United Kingdom* [2003] RJD 2003, App. No. 44647/98.

[177] *P.G. and J.H. v the United Kingdom* [2001] RJD 2001-IX, App. No. 44787/98.

[178] Ibid. § 57. See also: *Segerstedt-Wiberg and Others v Sweden* [2006] RJD 2006-VII, App. No. 44787/98 (in particular, § 72).

[179] *S. and Marper v the United Kingdom* [2008] RJD 2008, App. Nos. 30562/04 and 30566/04.

the rights of Article 8 of the ECHR.[180] In *S and Marper*, the applicants complained about the retention by UK authorities of their fingerprints, cellular samples and DNA profiles after criminal proceedings against them were terminated. The Court found that the three types of data deserved protection, but for different reasons.

Concerning cellular samples, the ECtHR noted that their retention had to be regarded 'per se' as interfering with the right to respect for private life, given the 'nature' (labelled as 'highly personal')[181] and the 'amount' of 'sensitive'[182] personal information they contained.[183] DNA profiles were described as containing less information, but as being able, nonetheless, to generate information going 'beyond neutral identification' (for instance, touching upon genetic relationships between individuals) when submitted to automated processing.[184] Finally, the storage of fingerprints was described as giving rise to important private-life concerns because they constituted data regarding identified or identifiable individuals held by public authorities with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes;[185] thus, not because of the nature of the data, but because of storage conditions.

The Strasbourg Court later affirmed in *Khelili*[186] that *Marper* had detailed some of the principles applying to the storage of 'personal' information, 'personal' being advanced here as in 'personal data protection':[187] the judgment was issued in French, and the words used by the Court (*à caractère personnel*)[188] were words ostensibly rooted in European data protection.[189] The qualification of data as 'personal' did not, however, trigger immediately the qualification of their memorisation as an interference under Article 8 of the ECHR: the Court declared that, in order to determine whether personal data engaged any aspects of private life, it was necessary to take into account the context in which the data had been collected and stored, their nature, the way they were used and treated and the results obtainable from the processing.[190]

The ECtHR case law built over the years upon *Leander* certainly appears to move towards the incorporation of the substance of Convention 108 into the

[180] See, for instance: (González Fuster 2009).

[181] *Marper* § 73.

[182] Ibid. § 72.

[183] Ibid.

[184] Ibid. § 75.

[185] Ibid. § 78–86. See also: (De Beer de Laer et al. 2010, p. 141).

[186] *Khelili v Switerland* [2011] App. No. 16188/07.

[187] See also, for references to both personal data and sensitive data as in Convention 108: *M.M. v UK* [2012] App. No. 24029/07 § 188.

[188] See, for instance, *Khelili* § 55.

[189] The case concerned a woman who contested her description as prostitute in a police database, and asked for the data to be rectified. In its assessment of whether there had been an interference, the ECtHR took notably into account the fact that the information was accessible in an automated database (§ 64).

[190] *Khelili* § 55.

interpretation of Article 8 of the ECHR. The degree of such incorporation is nevertheless debatable.[191] Ultimately, the case law evidences Strasbourg Court's reluctance to apprehend the assessment of whether a measure constitutes or not an interference with Article 8 of the ECHR in terms other than those present in that provision. The ECtHR has never declared that any automated processing of personal data shall per se be considered as an interference with Article 8 of the ECHR, but it remains unclear whether this should be interpreted as indicating that some processing activities are excluded from the scope of Article 8 of the ECHR (Kranenborg 2008, p. 1093), or, perhaps, simply not included yet.

4.3.3 Health Data

A category of data unquestionably portrayed by the ECtHR as deserving protection under Article 8 of the ECHR is data related to health. In this area, the ECtHR has been particularly keen to vocalise the importance of 'data protection', and of Convention 108. It is highly questionable, nonetheless, to which extent health data have been granted protection in the name of general 'data protection' (understood as the legal notion developed by Convention 108, applicable to any automated processing of personal data), or in the name of special provisions on special categories of data deserving reinforced protection (which are also covered by Convention 108).

An eloquent instance of these ambiguities is *Z v Finland*,[192] related to the disclosure of the medical condition of the applicant, who was infected with HIV, in the context of proceedings concerning a sexual assault. In its judgment, the ECtHR underlined that 'the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life' as guaranteed by Article 8 of the ECHR.[193] Despite this formal endorsement of 'the protection of personal data', eventually the Court justified the level of protection deserved by the information disclosed[194] not because it constituted 'personal data' in the sense of Convention 108, but because it was sensitive data, the disclosure of which 'may dramatically affect' the private and family life of individuals.[195] Additionally, the Court associated the protection in question with a principle 'of confidentiality',[196] and described it as consisting in safeguards to

[191] On the partial recognition of data protection under Article 8 of the ECHR by the ECtHR, see also: (De Hert and Gutwirth 2009, p. 24 ff).

[192] *Z v Finland* [1997] RJD 1997-I, App. No. 22009/93.

[193] Ibid. § 95. See also *M. S. v Sweden* [1997] RJD 1997-IV, App. No. 20837/92, § 51.

[194] In *Z v Finland*, the Court enters into these considerations when examining whether the interferences with Article 8 of the ECHR can be considered 'necessary in a democratic society'. It was undisputed that the various measures of which the applicant complained constituted interferences (*Z v Finland* § 71).

[195] Ibid. § 96.

[196] Ibid. § 95.

prevent some types of communication or disclosure,[197] even though 'data protection' in the sense of Convention 108[198] encompasses principles that go beyond confidentiality obligations.

I v Finland,[199] about the protection of patient records, added a new dimension to what is known as the doctrine of positive obligations in relation to the protection of personal data (De Hert 2009, p. 25). The case concerned an applicant, also diagnosed as HIV-positive, whose confidential patient records had been unlawfully consulted by her colleagues. The applicant complained that the district health authority had failed to provide adequate safeguards against unauthorised access of medical data. In this ruling, the ECtHR recalled that according to its own case law Article 8 of the ECHR does not merely compel States to abstain from interferences with the right to respect for private life, but that there may also be positive obligations inherent in an effective respect for private or family life,[200] and that these obligations may involve the adoption of measures designed to secure the respect for private life even in the sphere of the relations of individuals between them.[201]

4.3.4 Access to Data and Article 8 of the ECHR

Cases such as *Leander* and *Rotaru* concerned not only the storage of information by public authorities, but also the refusal to grant individuals access to the information stored,[202] thus depriving them of the opportunity to refute it.[203] Such refusal of access is also regarded by the ECtHR as an interference with the rights enshrined by Article 8 of the ECHR.[204]

A landmark judgment regarding access to information is *Gaskin*,[205] of 1989. In *Gaskin*, the applicant, who had been taken into care as a child, wished to find out about his past to overcome some personal problems, but had been refused access to his file on the ground that it contained confidential information. The Strasbourg Court found that the applicant had an essential interest in accessing the information at stake, described as relating to the applicant's childhood and formative years and, thus, to his 'private and family life', and eventually established there had been a violation of Article 8 of the ECHR because the decision on denial of access had not been taken by an independent authority (Sudre 2005, p. 409).

---

[197] Ibid.

[198] Some articles of which are expressly mentioned (in particular, Article 6 of Convention 108 on special categories of personal data), stating they are applicable *mutatis mutandis (Z v Finland § 95)*.

[199] *I. v. Finland* [2008] App. No. 20511/03.

[200] *Airey v Ireland* [1979] Series A No. 32, App. No. 6289/73, § 32.

[201] *X and Y v the Netherlands* [1985] Series A No. 91, App. No. 8978/80, § 23.

[202] See, for instance: *Leander* § 48.

[203] *Rotaru* § 46.

[204] See also: *M.G. v the United Kingdom* [2002] App. No. 39393/98.

[205] *Gaskin v the United Kingdom* [1989] Series A No. 160, App. No. 10454/83.

Some regard *Gaskin* as a leading case on the right of individuals, under Article 8 of the ECHR, to access information about them held by public authorities.[206] As a matter of fact, however, in that judgment the ECtHR did not focus its assessment on whether the information was *about* the applicant (in the sense of it being data related to him as an identified individual, or his 'personal data'), but rather on the issue of the impact on his life of not being able to access the information. The Court considered the refusal of access as amounting to an interference not because of the nature of the data, or of the way in which the data were used, but because of the denial of access' potential impact on the life of the applicant, and because the act of accessing the data served an essential interest. In this sense, the Court explicitly emphasised that its judgment shall not be interpreted as providing general guidance on the question of whether general access rights to personal information could be derived from Article 8 of the ECHR.[207]

4.3.5 Integration Through Article 8(2) of the ECHR

Further incorporation into the reading of Article 8 of the ECHR of principles related to the protection of personal data has been developed by the ECtHR in relation to the interpretation of the second paragraph of Article 8 of the ECHR, which describes the requirements for any interference to be legitimate (Nardell 2010, p. 46). In *Liberty*,[208] a case concerning the use of information gathered through the interception of communications, the Strasbourg Court detailed the substance of the requirement of legality (or of being 'in accordance with the law' as per Article 8(2) of the ECHR) in relation to further data processing of intercepted data (Nardell 2010, p. 46).[209] The Court notably connected the compliance with the legality requirement with the need to set out in detail rules on the storing and destroying of data, with a periodical assessment of the necessity to keep data stored, and with special supervision of these rules.[210]

In *S and Marper*, the ECtHR linked the application of personal data protection principles to the compliance with the requirement of measures being regarded as 'necessary in a democratic society'. In this sense, it framed data protection constraints as elements to be taken into account to assess whether data processing measures can be deemed proportional.[211]

[206] Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' 6 (1998) *International Journal of Law and Information Technology* 247.

[207] *Gaskin* § 37. See also: (Sudre et al. 2004, p. 343).

[208] Liberty and others v the United Kingdom [2008] App. No. 58243/00.

[209] On *Liberty* and legality, see also: (De Hert 2009, pp. 24–25).

[210] Liberty § 68.

[211] Ibid. 49. On proportionality, see also: *Segerstedt-Wiberg*, and (De Hert 2009, p. 26).

4.4 Summary

The activities of OECD and of the Council of Europe in the area of the regulation of data processing can be traced back to the 1960s, and are closely intertwined.

The main outcome of the OECD efforts was the adoption of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines are concerned with balancing the protection of the privacy of individuals with what was described as the 'free flow' of personal data across frontiers, even if such 'balancing' de facto privileges the promotion of such 'free flow' in the name of free trade. In the OECD context, national norms on the regulation of data processing are typically denominated 'privacy laws'.

The Council of Europe's main instrument is Convention 108, adopted in 1981. Convention's 108 basic approach can be synthesised as establishing a series of rules, labelled as 'data protection', which are presented as serving rights and freedoms in general, but, in particular, a right to privacy. In connection with Convention 108, national norms on data processing are 'data protection' rules, which serve (first and foremost) something called 'privacy'. The right to privacy pursued by data protection rules is, according to Convention 108, the right to respect for private life enshrined by Article 8 of the ECHR.

Under the direct influence of the OECD, Convention 108 echoed the notion of a 'free flow' of data, concretely as in 'free flow of information'. The notion's transposition into a Council of Europe's instrument marked a slight shift in its conception: it became now vaguely linked to the human right to freedom of expression.

The OECD Guidelines and Convention 108 promoted a way of framing the issues at stake that the ECtHR has only followed reluctantly. The ECtHR has over the years expanded its interpretation of Article 8 of the ECHR to encompass the protection of individuals in the face of some information practices, but has never openly and fully embraced the entire scope of application of Convention 108.[212] The Strasbourg Court has avoided the designation of any of the rights established by Article 8 of the ECHR as 'the right to privacy'. So, if it has confirmed by its practice of referring to Convention 108 when discussing Article 8 of the ECHR the perception that 'data protection' is related to the right to respect for private life, it has not clearly delimited how.

Convention 108 obliges ratifying countries to adopt their own legislation in accordance with its provisions. As a result, the notion of 'data protection' spread across Europe, and was notably championed by the UK, which adopted in 1984 its first Data Protection Act, after years of sterile deliberations on the possible acknowledgement of a right to privacy.

As they unfolded, the activities of the OECD and of the Council of Europe increasingly intersected with those of another organisation that began to be active in the field in the early 1970s: the European Communities, later known as the European Union. Chapter 5 is devoted to the involvement of the EU.

[212] Constituting what some have described as a 'somewhat confusing' case law (Bygrave (1998) op. cit. 17).

References

Arzt, Clemens. 2005. Data protection versus Fourth Amendment privacy: A new approach towards police search and seizure. *Criminal Law Forum* 16:183–230.

Bennett, Colin J., and Charles D. Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot: Ashgate.

Blackburn, Robert. 2001. The institutions and processes of the Convention. In *Fundamental rights in Europe: The European Convention on Human Rights and its Member States, 1950–2000*, eds. Robert Blackburn and Jörg Polakiewicz, 3–29. Oxford: Oxford University Press.

Blume, Peter. 1991. Introduction. In *Nordic studies in information technology and law*, ed. Peter Blume. Deventer: Kluwer.

Braibant, Guy. 1999. Introduction. *Revue française d'administration publique* 89 (janvier- mars) 5–8.

Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD). 2011. Modernisation of Convention 108: Proposals, Council of Europe Directorate General of Human Rights and Legal Affairs, T-PD-BUR (2011) 19_en, Strasbourg.

Bygrave, Lee A. 1998. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology,* 6, 247–284.

Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.). 2004. La protection de la vie privée et le traitement de données à caractère personnel. N°28. Bruxelles.

Commission nationale de l'informatique et des libertés (CNIL). 1982. Rapport au Président de la République et au Parlement 1980–1981, Prévu par l'art. 23 de la Loi du 6 Janvier 1978. La Documentation Française.

Commission on Human Rights of the United Nations Economic and Social Council. 1970. Human rights and scientific and technological developments: Report of the Secretary-General (Addendum 1). E/CN.4/102.

Committee of Ministers of the Council of Europe. 1981. Conclusions of the 336th meeting of the Ministers' Deputies held in Strasbourg from 9 to 11 September 1981, CM/DEL/CONCL(81)336, Strasbourg.

Committee on Legal Affairs and Human Rights. 1968. Human rights and modern scientific and technological developments, Doc. 2326.

Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). 2012. Final document on the modernisation of Convention 108, T-PD (2012) 04 Mos., Strasbourg.

Council of Europe's Consultative Assembly. 1949. First session, 10th August—8th September 1949, Part IV, Sittings 16–18, Strasbourg.

Council of Europe's Consultative Assembly. 1950a. Second session, II, 18th-24th November 1950, Reports Part V, Sittings 22–28, Strasbourg.

Council of Europe's Consultative Assembly. 1950b. Ordinary session 1950 (August 1950), Documents: Working papers, Part I, Doc. No. 1, Strasbourg.

Council of Europe's Consultative Assembly. 1953. Committee on General Affairs, fourth session, political review of the years 1945–1953, Documentary Note submitted by the Secretariat-General in relation to the report submitted by M. Spaak (Doc. AS/AG (5) 23) Strasbourg.

Council of Europe's Consultative Assembly. 1967. Eighteenth ordinary session (third part), 23rd–27th January 1967, Documents: Working Papers: Volume VI: Docs. 2160–2169, Strasbourg.

Council of Europe's Consultative Assembly. 1968. Nineteenth ordinary session (third part), 29th January–2nd February 1968, Official Report of Debates, Volume III, Sittings 577–948, Strasbourg.

De Beer de Laer, Daniel, Paul De Hert, Gloria González Fuster, and Serge Gutwirth. 2010. Nouveaux éclairages de la notion de "donnée personnelle" et application audacieuse du critère de proportionnalité, Cour Européenne des Droits de l'Homme, Grande Chambre, S et Marper c. Royaume Uni, 4 décembre 2008. *Revue trimestrielle des droits de l'homme* 81:141–161.

De Hert, Paul. 1998. Mensenrechten en Bescherming van Persoonsgegevens. Overzicht en Synthese van de Europese Rechtspraak 1955–1997. In *Jaarboek ICM 1997*. Antwerpen: Maklu.

De Hert, Paul. 2009. *Citizen's Data and Technology: An Optimistic Perspective*. The Hague: Dutch Data Protection Authority.

De Hert, Paul, and Serge Gutwirth. 2009. Data protection in the case law of Strasbourg and Luxem-bourg: Constitutionalisation in action. In *Reinventing Data Protection*?, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 3–44. Dordrecht: Springer.

De Hert, Paul, and Serge Gutwirth. 2013. *Anthologie de la vie privée*: *Compilation d'articles, de législation et de jurisprudence concernant la protection de la vie privée et des données à caractère personnel pour la Belgique jusque 1998*. Bruxelles: Academic and Scientific Publishers (ASP) & Commission Protection de la Vie Privée.

De Schutter, Olivier. 2001. Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel. *Revue trimestrielle des droits de l'homme* 45:148–183.

De Schutter, Olivier. 2010. *International Human Rights Law*. Cambridge: Cambridge University Press.

European Union Network of Independent Experts in Fundamental Rights. 2006. Commentary of the Charter of Fundamental Rights of the European Union.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press.

Gassmann, Hans Peter. 2010. 30 years after: The impact of the OECD Privacy Guidelines. Address to the OECD Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP). www.oecd.org/sti/interneteconomy/44945922.doc. Accessed 10 March 2013.

González Fuster, Gloria. 2009. TJCE—Sentencia de 04.12.2008, S. y Marper c. Reino Unido. *Revista de Derecho Comunitario Europeo* 33 (mayo-agosto): 619–633.

Hondius, Frits W. 1975. *Emerging Data Protection in Europe*. Amsterdam: North-Holland Publishing Company.

Hondius, Frits W. 1978. The Council of Europe's work in the area of computers and privacy (Discussion paper for the round table on the use of data processing for parliamentary work, Strasbourg, 18–19 May 1978). Strasbourg: Parliamentary Assembly of the Council of Europe.

Jacqué, Jean-Paul. 1980. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. *Annuaire Français de Droit International* 26:773–789.

Kirby, Michael Donald. 1980. International guidelines to protect privacy in transborder data flows. Australian & New Zealand Association for the Advancement of Science, Jubilee Congress, Adelaide, 15 May 1980.

Kirby, Michael Donald. 2010a. The OECD Privacy Guidelines @ 30. Organisation for Economic Co-operation and Development.

Kirby, Michael Donald. 2010b. The history, achievement and future of the 1980 OECD Guidelines on privacy. Presentation at round table on the 30th anniversary of the OECD Guidelines on privacy. Paris: Organisation for Economic Co-operation and Development.

Kranenborg, Herke. 2008. Access to documents and data protection in the European Union: On the public nature of personal data. *Common Market Law Review* 45 (4): 1079–1114.

Kuner, Christopher. 2011. Regulation of transborder data flows under data protection and privacy law: Past, present and future. OECD Digital Economy Papers No. 187. OECD Publishing.

Lageot, Céline. ed. 2008. *Dictionnaire plurilingue des libertés de l'esprit (Bruylant 2008)*. Bruxelles: Bruylant.

Lewis, Arthur. 1980. Opinion of the Committee on legal affairs and human rights on data processing and the protection of human rights, Doc. 4484.

Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.

Michael, James. 1994. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*. Aldershot: Dartmouth/UNESCO.

Nardell, Gordon Q. C. 2010. Levelling up: Data privacy and the European Court of Human Rights. In *Data protection in a profiled world*, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert, 43–52. Dordrecht: Springer.

Ooverkleeft-Verburg, Margriet. 1995. De Wet Persoonsregistraties Norm, toepassing en evaluatie. Tilburg: Katholieke Universiteit Brabant. http://www.overkleeft-verburg.nl/publicatiesproefschrift.htm. Accessed 10 March 2013.

Parliamentary Assembly of the Council of Europe. 1980. Report on data processing and the protection of human rights. (Rapporteur: Mr Holst), Doc. 4472.

Pavón Pérez, Juan Antonio. 2002. La protección de datos personales en el Consejo de Europa: El Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales. *Anuario de la Facultad de Derecho* 19–20:235–252.

Peers, Steve. 2006. *EU Justice and Home Affairs Law*. 2nd ed. Oxford: Oxford University Press.

Prieto Gutiérrez, Jesús María. 1998. La Directiva 95/46/CE como criterio unificador. *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* 23–26:1091–1173.

Registry of the Council of Europe. 1967. Travaux préparatoires de l'article 8 de la Convention européenne des droits de l'homme—European Court of Human Rights: Preparatory work on Article 8 of the European Convention on Human Rights (Bilingual Information Document), CDH (67) 5, Strasbourg.

Reidenberg, Joel, and Paul M. Schwartz. 1998. *Data Protection Law and On-Line Services: Regulatory Responses*. European Commission.

Robben, Frank, and Jos Dumortier. 1992. General consideration of the Belgian data protection bill of May 1991. In *Recent developments in data privacy law (ICRI N°2)*, 59–78. Leuven: Leuven University Press.

Simitis, Spiros. 2006. Einleitung: Geschichte—Ziele—Prinzipien. In *Bundesdatenschutzgesetz*, ed. Spiros Simitis, 61–153. Baden Baden: Nomos.

Sizer, Richard, and Philip Newman. 1984. *The Data Protection Act: A Practical Guide*. Aldershot: Gower.

Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz. 2006. *Information Privacy Law*. 2nd ed. New York: Aspen Publishers.

Sudre, Frédéric. 2005. *Droit européen et international des droits de l'homme*. 7th ed. Paris: Presses Universitaires de France.

Sudre, Frédéric, Jean-Pierre Marguénaud, Joël Andriantsimbazovina, Adeline Gouttenoire, and Michel Levinet. 2004. *Les grands arrêts de la Cour européenne des Droits de l'homme*. 2nd ed. Paris: Presses Universitaires de France.

The Privacy Protection Study Commission. 1977. *Personal privacy in an information society: The report of the Privacy Protection Study Commission*. Washington, D.C.: US Government Printing Office, 1977.

Working Party for Information Security and Privacy (WPISP). 2011. The evolving privacy landscape: 30 years after the OECD Privacy Guidelines. Directorate for Science, Technology and Industry—Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG(2010)6/FINAL,6.4.2011. DSTI/ICCP/REG(2010)6/FINAL.

Zerdick, Thomas. 1995. European aspects of data protection: What rights for the citizen? *Legal Issues of European Integration* 2:59–86.

Part II
In the European Union

Chapter 5
The Beginning of EU Data Protection

Everything flows.

(Teenage Fanclub 1990)

The European Union (EU) started to get involved in the regulation of data processing at the beginning of the 1970s. This chapter describes the initial steps of its involvement, and studies the crystallisation of EU legislation on (personal) data protection, up to the adoption of the EU Charter of Fundamental Rights in 2000. Chronologically, these developments partially overlap with those explored in the previous chapters, as well as with the evolution described in the following one, which traces the birth of the notion of EU fundamental rights, and examines its relationship with personal data protection.

5.1 Early Involvement

The European Economic Community (EEC), a component of the European Communities together with the European Coal and Steel Community, and with the European Energy Community, was founded in 1957 by six European countries: Belgium, France, Germany, Italy, Luxembourg, and the Netherlands. Later renamed European Community (EC) and absorbed into the European Union (EU), it has repeatedly accepted new members. In 1973, the United Kingdom (UK), Denmark and Ireland joined, followed by Greece in 1981, and Portugal and Spain in 1986. In 1995, Austria, Finland and Sweden acceded; in 2004, it was the turn of the Czech Republic, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia; in 2007, of Romania and Bulgaria; and, finally, in 2013, of Croatia.

The main institutions of the European Union are the Commission (through the years also known as Commission of the European Community, and European Commission), the European Parliament,[1] and the Council. The first two played an especially significant role in supporting EU's involvement in the field of data processing.

[1] On the role of the European Parliament in the development of EU personal data protection, see notably: (Bigo et al. 2011).

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_5,

More concretely, calls for action emerged in the context of the strengthening of the European computer industry.

5.1.1 Community Policy on Data Processing

By the beginning of the 1970s, both the European Commission and the European Parliament were concerned with United States (US) companies' dominance of the growing European market of computers and data processing.[2] To mitigate US market domination, in 1973 the Commission published a Communication to the Council, titled *Community policy on data processing*, suggesting it was necessary to devise systematic support for the development of the industrial application of data processing, which would help European industry to become globally more competitive (Commission of the European Communities 1973c).[3]

Describing complementary measures aimed at providing a favourable environment for a strong European data processing industry, and in order to support the effective application of computer systems, the Commission put forward in that 1973 Communication the need to adopt 'common measures for protection of the citizen' (Commission of the European Communities 1973c, p. 13).[4] In this context, the Commission's Communication noted that '(w)hen police, and tax, and medical records, and the files of hire purchase companies concerning individuals are held in data banks, the rules of access to this information become vital'; it argued that a wide debate on this matter was needed in the Community, and claimed that, '(i)n view of its basic constitutional importance', public hearings on the subject were desirable. The Commission, hinting that, in the absence of swift action at European level, divergent measures might be adopted by the Member Sates, also stressed that it was better for the Community to act quickly 'than to be obliged to harmonise conflicting national legislation later on' (Commission of the European Communities 1973c, p. 13).

Several features of the 1973 Communication announced already characteristic features of later EU developments: first and foremost, it is noticeable that the main argument advanced by the European Commission to call for action was the necessity to avoid the surfacing of divergent, or conflicting, national laws. Second, it is also noteworthy that the Commission underlined the 'constitutional importance' of the issue—despite the fact that by 1973 there were no constitutional provisions on data processing in any European country (yet). At this time, in any case, the

[2] See, for instance: (Commission of the European Communities 1972).

[3] See also: (Commission of the European Communities 1973b). The responsible Commissioner for Industrial Affairs, General Research and Technology and the Joint Research Centre (JRC) was at the time Altiero Spinelli.

[4] The need to consider the link between concrete initiatives related to support of the data processing sector and policy in general had already been advanced in another document, the 1973 Commission's *Scientific and Technical Policy Programme* (Commission of the European Communities 1973a).

Commission failed to adopt any particular terminology to refer to the kind of provisions discussed, alluding simply to 'rules of access' to information about individuals held in data banks.

The Commission's recommendations on launching a wider debate on these 'rules of access' to information about individuals were basically ignored by the Council. And they initially generated very limited interest at the European Parliament. In March 1974, however, a French Member of the European Parliament (MEP), Pierre Bernard Cousté, submitted an oral question to the Council on the subject of '(p)rotecting the privacy of the Community's citizens'.[5] Cousté was presumably particularly interested in the issue in the context of his own participation to the response, in France, to the public outcry generated by revelations concerning the S.A.F.A.R.I. project.[6] As a matter of fact, only a few days after having submitted his oral question to the Council on citizens' *vie privée*, he introduced a legislative proposal on the same issue in France.

Cousté's parliamentary question took note of the fact that many large data banks were already operational or being set in different EC countries, and inquired whether the Council would propose to take measures within the framework of Community data processing policy 'to protect and guarantee the privacy of citizens, in particular by strictly regulating conditions for access to such information'.[7] His question thus associated the notion of rules on access to personal information with the word privacy (*vie privée*).

The competent representative of the Council replied to Cousté's question in a sitting of the European Parliament still in March 1974.[8] In his answer, he observed that the Council had not made any official statement following the Commission's 1973 Communication on *Community policy on data processing,* nor had it been requested to do so, and expressed that it was thus premature to deliver any opinion on the subject; nevertheless, he maintained that the ultimate interrogation to be considered was whether the protection of the private life of the individual required Community legislation, or whether it could be left in the hands of Member States.[9] The debate following this intervention illustrated some of the different national sensitivities of the time, as well as diverse national terminological stances: some deputies called for the Council to urge Member States to adopt 'data protection laws',[10] while others argued that 'a right to privacy' should be defined at the level of the EC.[11] During his

[5] Oral question No 193/73 with debate, pursuant to Rule 47 of the Rules of Procedure by Mr Cousté on behalf of the Group of European Progressive Democrats to the Council of the European Communities [1974] OJ C40/21.

[6] See Chap. 3, Sect. 3.1.4, of this book.

[7] Ibid.

[8] The name of the Council representative was Mr Apel. The sitting took place on 13 March 1974 (General Secretariat of the Council of the European Communities 1974, p. 14).

[9] Oral Question No. 193/73, with debate, on protecting the privacy of the Community's citizens, OJ Debates of the European Parliament No 173 (March 1974) 35.

[10] Ibid. 36 (in line with German terminology).

[11] Ibid (in line with approaches discussed at the time in the UK).

concluding remarks, Cousté announced that the European Parliament's Committee on Economic and Monetary Affairs was preparing a report on EC policy on data processing,[12] in which the issue would be further considered.

The Committee on Economic and Monetary Affairs of the European Parliament was indeed working on the subject, and, in this context, had heard EC Commissioner Altiero Spinelli. In his statement before the Committee, however, Commissioner Spinelli apparently missed the opportunity to deal with 'the problems connected with the protection of citizens in view of the increasing use of data-processing by public and private concerns' (Spinelli 1974, p. 1), and, consequently, he decided to send a letter to the President of the European Parliament to discuss this subject more in detail.

In such follow-up letter, dated 21 March 1974, Spinelli pointed out that both Member States and international organisations such as the OECD were studying the question of the protection of citizens and data processing, and declared that '(t)he Commission realizes that the communication of data across frontiers will be a European problem likely to require harmonization' (Spinelli 1974, p. 2). He stated, however, that '(g)iven the constitutional importance of the problem', the European Commission considered that it would be expedient for the European Parliament to take care of discussing the matter in depth, and even suggested that an ad hoc committee should be set up at the European Parliament to organise a series of public hearings (Bureau du Parlement Européen 1974, p. 16). Spinelli's letter included an annex on 'The problem of data-banks and protection of the freedom of the individual' with concrete suggestions for the composition and work of the recommended parliamentary committee, as well as a list of 'major aspects requiring analysis and/or policy decisions', including a review of the legislative situation in Member States, solutions discussed 'in the leading industrialized countries', the problem in relation to the ECHR, and a definition of a common basis for future legislation (Spinelli 1974, p. 3). In addition, the Vice-President of the Commission himself later contacted the Bureau of the European Parliament to express that due to the eminently political character of the subject of data banks and the protection of the individual, the European Commission felt it was suitable that the European Parliament engaged with the issue (Bureau du Parlement Européen 1974, p. 17).

MEPs appeared generally unconvinced by the Commission's suggestion that the European Parliament was to take the lead in this area. During internal discussions, it was pointed out that although the European Parliament might contribute to the substantive debate, the collection of facts and information on the basis of which could be put forward any Community legislation was a task more suited for the Commission.[13] There were also some tensions regarding who could be entrusted with

[12] Ibid.

[13] Legal Affairs Committee of the European Parliament, Interim Report drawn on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing (Rapporteur: Lord Mansfield), Working Documents 1974–1975, Document 487/74, PE 39.608/fin, 19.2.1975, p. 14.

making progress inside the European Parliament,[14] as the Committee on Economic and Monetary Affairs, responsible for the follow up of EC industrial policy in the context of which had emerged the question at data processing, did not seem particularly eager to start dealing with issues of privacy or data protection. Nonetheless, in July 1974, Commissioner Spinelli insisted again on the fact that the Commission wished that the EP examined the matter and expressed its views.[15]

In October 1974, the Legal Affairs Committee of the European Parliament was finally authorised to prepare a report on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing, to be formally presented as an 'own initiative' report, even if substantially linked to the Commission's 1973 Communication on *Community policy on data processing*.[16] In November 1974, the Legal Affairs Committee appointed Lord Mansfield[17] as responsible rapporteur.[18]

5.1.2 The 1975 and 1976 Resolutions of the European Parliament

In February 1975, based on the report prepared by Lord Mansfield, the European Parliament adopted a *Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*,[19] where MEPs manifested that they considered an urgent necessity the adoption of a Directive on 'individual freedom and data processing'.[20] The Directive should aim at preventing the development of conflicting legislation among Member States, as advanced by the European Commission in its 1973 Communication, but also at ensuring the maximum level of protection of Community citizens. The European Parliament simultaneously gave its approval to the establishment of a special committee of MEPs to consider proposals relating to, inter alia, the rights of the individual in relation to information stored in data banks, and the effective application of sanctions for infringement of 'individual privacy'.[21]

In his report preceding the 1975 Resolution, Lord Mansfield had explained that Member States were already active in this field, referring in particular to the German federal state of Hesse's experience of 'parliamentary control of electronic data

[14] Ibid.

[15] Ibid.

[16] Ibid. p. 3.

[17] William David Murray, 4th Earl of Mansfield and Mansfield.

[18] PE 39.608/fin, p. 11.

[19] Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing [1975] OJ C60/48.

[20] Ibid. paragraph 1.

[21] Ibid. paragraph 2.

banks',[22] as well as to proposals for legislation made in Germany, Belgium and the UK, to the studies carried out by the OECD, and to the Resolutions adopted by the Council of Europe in 1973 and 1974.[23] The rapporteur stressed that the objective of the European Parliament's involvement in the area should not be to achieve 'an overall definition of the right of personal privacy',[24] but rather to examine 'the more restricted field of intrusion on privacy by misuse of automatic data processing techniques'.[25] In his view, taking into account that the European Parliament had consistently sought to defend the rights of EC citizens, it should accept willingly the opportunity to make a positive contribution to the EC legislative processes to counter the dangers of misuse of advanced methods of mechanisation and computer technology when applied to the collection, storage, collation and distribution of personal information.[26]

Neither the Commission nor the Council undertook any particular action in direct response to the European Parliament's 1975 Resolution. A year later, in April 1976, the European Parliament adopted a second *Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*,[27] expressing it was 'anxious to continue and step up its activities as regards the protection of the rights of the individual',[28] and that it was aware of the public concern caused by the risks of misuse or abuse of information stored in data banks. Emphasising that several Member States had already started to draft laws in the field,[29] and in order to guard against the adoption of conflicting national laws, MEPs requested the Commission to start working on the drafting of EC legislation.[30] The Resolution also formally instructed to report on the issue the EP Legal Affairs Committee,[31] which appointed as rapporteur Mr Bayerl, who, in his turn, proposed to set up a special Sub-Committee at the European Parliament to address the question.[32]

This special Sub-Committee was called the Data Processing and Individual Rights Sub-committee, and worked on the subject from June 1977 to March 1979. It notably organised a public hearing on the processing of data and the rights of the

[22] PE 39.608/fin, p. 7.

[23] Ibid. The report also mentions progress in the US (ibid. p. 12).

[24] PE 39.608/fin, p. 7.

[25] Ibid.

[26] Ibid. p. 9.

[27] Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing, OJ [1976] OJ C100/27.

[28] Ibid.

[29] Although Sweden had already adopted a national-level data protection instrument, it was not a Member State of the EC at the time.

[30] Ibid.

[31] Ibid.

[32] European Parliament, Report drawn up on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of technical developments in data processing (Rapporteur: Mr A. Bayerl), Working Documents 1979–1980, Document 100/79, 4.5.1979, p. 3.

individual in 1978, which was attended by experts and observers from the OECD, the Council of Europe, and the EC Commission.[33] In a questionnaire prepared for the public hearing, the Sub-Committee notably inquired whether it would be necessary for the control of data protection inside the EC to establish a distinct authority. Experts answered rather reticently (Burkert 1979, p. 201).

The Sub-Committee heard evidence from the Rheinland-Pfalz Data Protection Commission, as well as from the *Datenschutzbeauftragter* of Hessen, Spiros Simitis, and visited the Swedish Data Inspection Board, even though Sweden was not a Member State yet. On the basis of the information gathered, the Sub-Committee elaborated a report, known as the Bayerl Report, reviewing the developments in the field in the Member States of the European Communities, as well as in a selected number of Members of the Council of Europe, and of the OECD. The report significantly noted that Austria (also still not an EC Member State), with its Federal Data Protection Law of 1978, had afforded individuals 'a Constitutional right of personal data secrecy'.[34]

5.1.3 Commission's First Steps

In the meantime, the EC Commission had launched informal discussions with Member States on a possible harmonisation of European legislation (Commission of the European Communities 1976, p. 8), and its Directorate-General for Industrial and Technological Affairs established a Working Party on Data Processing and Protection of Liberties. In 1976, the Commission declared that 'the protection of the citizen's privacy' had been recognised as a matter of EC interest since 1973, and stressed that citizens' rights in the field were becoming 'a constitutional issue significant in the context of European union' (Commission of the European Communities 1976, p. 8). The EC Commission viewed privacy as very closely linked to the question of 'data security and confidentiality', portraying a proposal to launch a study on this specific issue as a direct response to European Parliament's calls for new EC legislation on privacy (Commission of the European Communities 1976, p. 13).

EC activities in the area unfolded at this time mainly through the funding of studies. In September 1977, the Council decided to support research to promote the use of 'informatics',[35] including a three-year study on data security and confidentiality. The Commission was made responsible for carrying out the study, assisted by an Advisory Committee on Joint Data Processing Projects, and the study's object was described as: 'to examine, in conjunction with the Committee of National Experts convened by the Commission, the chief problems relating to the harmonization of

[33] Ibid. p. 13. The public hearing took place in Brussels on 6 February 1978.

[34] Ibid. p. 18.

[35] Council Decision of 27 September 1977 adopting a series of studies in support of the use of informatics (77/616/EEC) [1977] OJ L255/25.

Community legislation covering the protection of private life and the development of codes of application and corresponding standards'.[36] The Council explicitly specified that the research should include the 'analysis of studies undertaken at national level in the Member States and other countries such as Sweden and the United States'.[37]

Three institutions worked together to carry out the study: the German Gesellschaft für Mathematik und Datenverarbeitung (GMD), the French Institut national de recherche en informatique et en automatique (INRIA), and the British National Computing Centre (NCC). Their research was updated until September 1979 (Burkert 1979, p. 5),[38] and included thus a reference to the fact that, in Germany, a Federal Data Protection Act had entered into force in January 1978 (Burkert 1979, p. 100). In its review of existing legislation, the investigation highlighted the interrelations between different national developments, underscoring that many national approaches had been developed taking into account the pioneering Swedish example, and that, in general, there was a tendency to be mindful of experiences elsewhere, as well as to search for common strategies—for instance via the Council of Europe, the OECD, or the European Communities (Commission of the European Communities 1982, p. 8). The study also pointed out that Belgium, the UK[39] and the Netherlands had not yet adopted any legislation, but had nonetheless issued bills or studies on the subject, whereas in Italy and Ireland there was no official document on the matter (Commission of the European Communities 1982, p. 5). The inquiry devoted much attention to some specific differences between existing approaches, in particular to the question of whether legislation should apply to moral persons (Bancilhon et al. 1979).[40] As this study was being completed, the European Parliament adopted a new resolution on the protection of individual rights and data processing.

5.1.4 The 1979 Resolution of the European Parliament

In May 1979, on the basis of the *Bayerl report* and of the work of the Sub-Committee described above, the European Parliament adopted a *Resolution on the pro-*

[36] Ibid. p. 26. The study was grounded on the idea that 'the development of informatics applications calls for an examination of the problems of data security and confidentiality and of the technical, legal and social aspects thereof, in particular with a view to protecting citizens in respect of the use of informatic facilities' (ibid. p. 25).

[37] Ibid. p. 26.

[38] See also: (Commission of the European Communities 1982, p. 7).

[39] In the UK, the Lindop Report was being discussed (Commission of the European Communities 1982, p. 5).

[40] The study noted that among laws adopted and entered in force, only the laws from Austria, Norway and Denmark protected in the same way the data related to physical persons and the data concerning moral persons, but that Luxembourg had aligned itself in that sense too (Bancilhon et al. 1979, p. 2). The authors also stressed that, during negotiations for the OECD Guidelines, US representatives had strongly opposed the idea of extending protection to the data related to moral persons, arguing there was no necessity (Bancilhon et al. 1979, p. 3).

tection of the rights of the individual in the face of technical developments in data processing.[41] The document reverberated the European Parliament's Resolutions of 1975 and 1976, except that this time the institution formally broadened its scope of concern to the protection of rights in face of developments in data processing in general, and not only in relation to automated data processing.

In the 1979 Resolution, the European Parliament remarked that Member States had already started to adopt 'national provisions to protect privacy',[42] and underlined that this could have a negative impact on the development of the common market, and on the creation of 'a genuine common market in data-processing' requiring the insurance of 'the free movement of information within the Community'.[43] The European Parliament called for the strengthening of the Community's participation in all international forums dealing with these issues, and stressed it was necessary to consider the possible accession of the Community to the ad-hoc Convention that was yet to be adopted by the Council of Europe.[44] It also restated its demands to the Commission to prepare a Directive harmonising legislation on data protection.[45] In the European Parliament's view, EC institutions were clearly empowered to take action in this field, as long as they conformed with the principles of the Joint Declaration on the Protection of Fundamental Rights adopted in 1977 by the European Parliament, the Council and the Commission to stress the prime importance they attached to the protection of fundamental rights.[46]

The 1979 Resolution included a series of recommendations describing substantive principles that, according to the European Parliament, needed to form the basis of any future Community norms in the field.[47] The principles consisted of a series of obligations imposed on 'data controllers' when processing data,[48] rights to be granted to '(a)ll persons whose usual residence is in the territory of a Member State' in relation to the processing of data relating to them,[49] and norms on the existence of national independent bodies to monitor compliance with the applicable rules, as well as on the creation of a 'data control body of the European Community', composed of representatives of national bodies, and chaired by a European Parliament representative.[50]

---

[41] Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing [1979] OJ C140/34.

[42] Ibid. p. 35.

[43] Ibid.

[44] Ibid. p. 36.

[45] Ibid. p. 35.

[46] Ibid. p. 36.

[47] *Recommendations from Parliament to the Commission and Council pursuant to paragraph 10 of the motion for a resolution concerning the principles which should form the basis of Community norms on the protection of the rights of the individual in the face of developing technical progress in the field of data processing* (ibid. p. 37).

[48] Ibid. Sect. I of the Recommendations.

[49] Ibid. Sect. II of the Recommendations.

[50] Ibid. p. 38 and 36 (in particular, paragraphs 13 and 14).

MEPs also continued to put pressure on the Commission by presenting oral questions. In 1979, there was a debate at the European Parliament following the introduction of an oral question entitled *Data protection in the Community*,[51] addressed to the Commission. The question inquired on the remedies available to the citizen against improper use of nationally protected data in the territory of the Community in cross-frontier traffic, and on the Commission's attitude towards the setting up of an official international or Community body to control the cross frontier transmission of data.[52] One of the co-authors of the question, Mr van Aerssen, explained that its purpose was to make sure that the results of the old Parliament's endeavours in the field did not go unrecognised in the new Parliament.[53] In this sense, he stressed that 'the former European Parliament devoted close attention to the problem of data protection'.[54] In his reply, the Vice-President of the Commission, Mr Natali, stated that the Commission was 'perfectly aware of the need for international rules for the protection of personal data'.[55] Nevertheless, he added that the Commission preferred 'to see how the situation develops in the Council of Europe'.[56] The Commission thus appeared to be waiting for the results of the work undertaken by the Council of Europe, the outcome of which was Convention 108.

In 1981, after the adoption of Council of Europe's Convention 108, the European Commission asserted that, in its view, Convention 108 was an appropriate instrument for the purpose of creating a uniform level of data protection in Europe.[57] Hence, it published a Recommendation inviting all Member States to ratify Convention 108 as soon as possible, and, in any case, before the end of 1982.[58] Arguing that the approximation of national laws in this area was a necessity, the Commission noted that, if Member States failed to observe these recommendations, it could propose the adoption of a Community instrument to achieve the same aim.

In this 1981 Recommendation, the European Commission explicitly announced that data protection had the quality of fundamental right,[59] except to the readers of the English version. Indeed, although the Recommendation's Dutch version expresses that data protection *'heeft het karakter van een grondrecht'*, even if the German version proclaims that it *'hat den Charakter eines Grundrechts'*, despite the fact that the French text promulgates that '*elle a le caractère d'un droit fondamental'*, and notwithstanding that the Italian one maintains that it '*riveste il*

[51] Data protection in the Community: Oral question with debate (Doc. 1-287/79) by Mr van Aerssen and Mr Alber [1979] OJ Debates of the European Parliament No 245 (September 1979) 15–26.

[52] Ibid. p. 19.

[53] Ibid.

[54] Ibid.

[55] Ibid. p. 20.

[56] Ibid.

[57] Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31, recital 5.

[58] Ibid. p. 31.

[59] Ibid paragraph 2 of Sect. I.

carattere di un diritto fondamentale", the English version merely concedes as follows: 'Data-protection is a necessary part of the protection of the individual. It is quite fundamental'.[60]

As this Recommendation was made public, more discreet work towards the eventual preparation of EC legislation on data protection continued to develop. The study on data security and confidentiality that the Commission had announced in 1976 was finally concluded in 1979, and was discussed by a Group of Experts on Data Processing and the Protection of Personal Liberties in 1980. The Commission, in agreement with the Group of Experts, identified additional sub-subjects requiring further research,[61] and launched follow-up initiatives.[62]

In March 1982, the European Parliament adopted a new *Resolution on the protection of the rights of the individual in the face of technical developments in data processing*,[63] where it also welcomed the adoption of Convention 108, called on to all Member States to sign it and ratify it as soon as possible, and advocated again for the direct accession of the Community to the Convention. Contrary to the Commission, however, the European Parliament argued that, in spite of the existence of Convention 108, and regardless of its eventual ratification by all Member States, it was still necessary to adopt Community rules on data protection, in particular based on Article 100 of the EEC Treaty—thus, in order to contribute to the establishment of the common market.[64] In this 1982 Resolution, the European Parliament also expressed its support for 'investigating the possibility and desirability of expressly incorporating the right to the protection of personal data as a human right or fundamental freedom' in the text of the ECHR.[65]

Up to mid 1980s, the European Community continued to promote studies related to 'data protection' in the context of its support for data processing. In April 1984,[66] the Council expressed commitment to co-finance, under the label of research on 'confidentiality and data security', studies with the aim of examining 'legislation in force or in preparation in the Member States and discussion

[60] Ibid.

[61] The quality and quantity of cross-frontier data flows; the organisational character and technical functioning of data protection bodies; the problem of legal personality (individual and legal entities); the technical aspects of the right of access to data-registers; and the control, audit and implementation of requirements relative to confidentiality and their impact on data security (Commission of the European Communities 1982, p. 7).

[62] It was agreed that shall be studied in particular the protection of data in the light of the new information and communication technologies; technologies applicable to data protection and security; personal data and the automatic decision-making process; the impact of international data protection regulations on sectors most concerned with information; system design and data protection; freedom of access to information and data protection; data banks, distributed systems and data protection (Commission of the European Communities 1982, p. 30).

[63] Resolution of the European Parliament of 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing [1982] OJ C87/39.

[64] Ibid. p. 40.

[65] Ibid.

[66] Council Decision of 10 April 1984 amending Decision 79/783/EEC adopting a multiannual programme (1979 to 1983) in the field of data processing (84/254/EEC) [1984] OJ L126/27.

of harmonization possibilities and of instruments which might be implemented at Community level'.[67]

5.1.5 EU Data Protection Emerging Outside EC Law

As a matter of fact, the first concrete moves towards integration of 'data protection' in the sense of Convention 108 into EU policy and EU law were originally undertaken outside the institutional framework of the European Communities. They occurred in the context of intergovernmental cooperation between Member States in the field of Justice and Home Affairs. The original Treaties did not contain provisions conferring powers to the Community in this area, so when cooperation between Member States began (and it did already in the 1970s) it mainly took place at the margins of the Council (Piris 2010, p. 167).

A major initiative in this context was the Schengen Agreement, a treaty on the gradual abolition of checks at internal borders signed in 1985 by five of the Member States of the European Community: Belgium, France, Germany, Luxembourg and the Netherlands.[68] The Schengen Agreement entered into force in 1986, but conditioned the actual lifting of borders (the abolition of border checks) to the adoption of 'compensatory measures' (Piris 2010, p. 169), essentially detailed in a Convention implementing the Schengen Agreement concluded by the same Member States in 1990.[69]

The 1990 Convention established a 'joint information system', the Schengen Information System (SIS), consisting of interconnected national sections to which all parties were to have access via an automated search procedure, including alerts on persons and property.[70] The Convention devoted a whole Chapter to the 'Protection of personal data and security of data' in the SIS,[71] setting up the obligation for Contracting Parties to adopt national provisions ensuring at least a level of protection

[67] Ibid. p. 31. In November 1984, nonetheless, the Council decided that further studies on 'confidentiality and data security' would be devoted to 'the confidentiality and security of data and software with a view of developing tools for users' (Council Decision of 22 November 1984 amending Decision 79/783/EEC in respect of general measures in the field of data processing (84/559/EEC) [1984] OJ L308/49). Among such tools was identified a 'Data protection guide for European users', 'data protection' being understood in this context as a technical feature applicable to data (*Call for proposals for projects relating to the security and protection of data, the protection of computer programs and the vulnerability of the information society (85/C 204/02)* in Commission Communication in the field of data processing: Notice of a call for proposals for projects relating to the security and protection of data, the protection of computer programs and the vulnerability of the information society (85/C 204/02) [1985] OJ C204/2).

[68] On Schengen cooperation and the protection of personal data, see, notably: (E. Brouwer 2008).

[69] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 19 June 1990.

[70] Article 92 of 1990 Schengen Convention.

[71] Ibid. Chap. 3.

equal to the level granted by Convention 108,[72] which had entered into force in 1985. National legal systems were also obliged to comply with principles approved by the Committee of Ministers of the Council of Europe specifically for the use of personal data in the police sector in a Recommendation adopted in 1987.[73]

The Convention implementing the Schengen Agreement required the establishment in each participating country of an independent national supervisory authority, responsible for carrying out supervision of SIS national sections, and for checking that data processing does not violate the rights of the data subject.[74] All individuals were given the right to ask national supervisory authorities to check the data entered in the system,[75] and to have access to data entered in the SIS relating to them, to be exercised in accordance with national laws.[76] Participant countries were given the possibility, however, to leave in the hands of the national supervisory authority the decision on whether the requested information shall be communicated to the individual.[77] All persons were recognised the right to have deleted data factually inaccurate, as well as unlawfully stored data relating to them.[78]

The 1990 Convention detailed specific obligations applicable to personal data in the SIS, such as the requirement to keep data entered for the purposes of tracing persons stored only for the time required to meet that original purpose,[79] or security requirements.[80] Additionally, a joint supervisory authority, consisting of two representatives from each national supervisory authority, was set up to supervise the technical support function of the SIS.[81] The 1990 Convention did not mention any right to privacy, or to private life,[82] or fundamental rights and freedoms.[83]

[72] Ibid. Article 117. See also Article 126.

[73] Recommendation No R (87) 15 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, adopted on 17 September 1987). See Article 129 of 1990 Schengen Convention.

[74] Article 114(1) of 1990 Schengen Convention.

[75] Ibid. Article 114(2).

[76] Ibid. Article 109(1).

[77] Communication of information to the data subject shall in any case be refused if indispensable for the performance of a lawful task in connection with the alert, or for the protection of the rights and freedoms of third parties, and, in any event, during the period of validity of alerts for the purpose of discreet surveillance.

[78] Ibid. Article 110. Qualifying them as 'well established' rights: (Zerdick 1995, p. 71).

[79] Article 112(1) of 1990 Schengen Convention.

[80] Ibid. Article 118.

[81] Ibid. Article 115.

[82] The 1990 Convention mentioned 'private homes' when establishing that officers carrying out certain surveillance measures were in any case not entitled to enter 'into private homes and places not accessible to the public' (Article 40(3)(e) of 1990 Schengen Convention).

[83] The 1990 Convention referred only to the protection of the rights and freedoms of third parties as a legitimate ground to refuse communication of information to the data subject (Article 109(2) of 1990 Schengen Convention).

5.2 Developing EC Data Protection Law

The key step towards the adoption of Community legislation on data protection took place in 1990, when the European Commission adopted a package of proposals related to the protection of personal data, in the form of a Communication (Commission of the European Communities 1990).[84] The package included a Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data,[85] a proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks,[86] a request for a mandate to negotiate with the Council of Europe in order to adhere to Convention 108,[87] a Declaration to the effect that the institutions of the European Community will accept to apply the same principles as introduced in the general Directive for the files which they hold themselves,[88] a draft Resolution of the representatives of the governments of the Member States meeting in the context of the Council to extend the application of the general Directive to those personal data files which do not fall within the scope of Community law,[89] and a Proposal for a Council Decision on information security.[90]

5.2.1 Directive 95/46/EC

The Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data was to become the main Community instrument for the protection of personal data, when it was approved five years later.

---

[84] Hereafter, COM(90) 314 final. The proposals were also published, without explanatory memorandums, in: [1990] OJ C277/1. On the Communication, see: (Papapavlou 1992).

[85] *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data* (SYN 287). The proposal was transmitted to the Council on 27 July 1990, and to the European Parliament on 3 October 1990.

[86] *Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks* (SYN 288).

[87] *Recommendation for a Council Decision on the opening of negotiations with a view to the accession of the European Communities to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data.*

[88] *Commission Declaration on the application to the institutions and other bodies of the European Communities of the principles contained in the Council Directive concerning the protection of individuals in relation to the processing of personal data.*

[89] *Draft Resolution of the Representatives of the Governments of the Member States of the European Communities meeting within the Council.*

[90] *Proposal for a Council Decision in the field of information security.*

5.2.1.1 Legislative Process

In the 1990 Communication, the EC Commission argued that it was necessary to introduce Community measures for the protection of individuals in relation to the processing of personal data because the diversity of national approaches endangered European integration.[91] The Commission noted that disparities included differences in relation to the scope of norms (concerning the applicability to manual processing, or the applicability to legal persons), and to the preconditions for processing (obligations to notify, information obligations at the time of collection, processing of sensitive data),[92] and that Convention 108 had failed to have any substantial impact on reducing them. Evoking previous requests to work on the approximation of laws in this field, the Commission mentioned the repeated calls in this sense voiced by the European Parliament.[93]

According to the Commission, the aim of national laws in the field was 'to protect the fundamental rights of individuals, and in particular the right to privacy'[94]—which was, in reality, not the explicit purpose of any existing national law, but rather of Convention 108. The 1990 draft Proposal for a Council Directive highlighted as one of its objectives 'the protection of the privacy of individuals in relation to the processing of personal data contained in data files'[95] (without referring to any other rights and freedoms), and portrayed 'privacy' as being recognised in Article 8 of the ECHR (in line with Convention 108), as well as in the general principles of Community law.[96] The explanatory memorandum introducing the text incidentally recalled that, in a 1981 Recommendation, the Commission had stated that data protection 'is quite fundamental',[97] but the English version of the text ignored any reference to its quality of *fundamental right* alluded to by the non-English versions of the previous text.[98]

The Commission stressed that because of its own commitment to fundamental rights, it could only promote a high level of protection of these rights. And it argued that, by insuring such high level of protection by a Community system, it would remove obstacles to the establishment of the internal market in accordance with Article 100a of the EC Treaty.[99] The second major objective of the Proposal was thus to prevent restrictions to 'the free flow of personal data between Member States'.[100]

---

[91] COM(90) 314 final, p. 2.

[92] Ibid. p. 3.

[93] Ibid.

[94] Ibid. p. 5.

[95] Article 1(1) of 1990 draft Proposal.

[96] Recital 7 of 1990 draft Proposal.

[97] COM(90) 314 final, p. 13.

[98] The French version of the Communication, nevertheless, points out that the Commission had previously noted that data protection had the quality of a fundamental right (COM(90) 314 final, p. 14).

[99] Ibid. p. 5.

[100] Article 1(2) of 1990 draft Proposal.

The 1990 Communication therefore already delineated the two main (and, for some, contrasting)[101] elements of what was to become the final 1995 Directive: a fundamental rights dimension, and an internal market facet.[102] The internal market dimension of the Proposal and the identification of Article 100a of the EC Treaty as the appropriate legal basis for its adoption[103] were regularly stressed by the Commission, whose competence to propose legislation in this area was at that time often contested due to its lack of any general power to propose rules on human rights (Coudray 2010, p. 31). The 1986 Single European Act,[104] which had entered into force on 1 July 1987, fixed as deadline for the completion of the internal market the year 1992, and was thus at the time a priority.

The Proposal addressed four main issues: the conditions under which the processing of personal data is lawful, the rights of data subjects, the requisite of data quality, and, in response to demands by the European Parliament for the creation of a consultative body at Community level (Guerrero Picó 2006, p. 62), the setting-up of a Working Party on the Protection of Personal Data to advise the Commission on data protection issues.[105] The Proposal covered both the private sector and the activities of the public sector falling within the scope of Community law,[106] although it advanced different rules for each. The text was very much influenced by Convention 108 and by the German Federal Data Protection Act, and, to a lesser extent, by the French *loi informatique et libertés* (Guerrero Picó 2006, p. 61; Heil 2010, p. 10). The similarities to Convention 108 were not accidental, as the Commission had been following closely its drafting, as well as its implementation, and had even agreed in 1989 to finance a study commissioned by the Consultative Committee set up under Convention 108 on possible clauses for inclusion in a model contract to ensure equivalent protection in the context of transborder data flows (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data 1992, p. 5).

The right to privacy was mentioned not only among the basic objectives of the Proposal, but also in a provision establishing that 'data files falling exclusively with the confines of the exercise of a natural person's right to privacy, such as personal address files' should be excluded from protection.[107] The right was also used to characterise 'sensitive data', or 'data which are capable by their very nature of

[101] Referring to divergent interests: (Büllesbach et al. 2010, p. 3).

[102] Ibid. p. 6. The Commission also made a reference to a need, previously mentioned by the Council, to ensure that cooperation between administrations promoting the free movement of persons granted protection to individuals with regard to the use of 'personalized data banks' (COM(90) 314 final, p. 4).

[103] Ibid. p. 17.

[104] Single European Act [1987] OJ L169/1.

[105] COM(90) 314 final, p. 12.

[106] Ibid.

[107] Recital 9 of 1990 draft Proposal.

infringing the right to privacy', which, it was maintained, should be granted reinforced protection.[108]

The legislative procedure applicable to the draft Proposal imposed the consultation of the Economic and Social Committee, which delivered its Opinion on the text in April 1991.[109] In its Opinion, the Economic and Social Committee criticised the draft for identifying as one of its objectives the protection of privacy without mentioning other rights and freedoms, taking into account that its preamble referred to the ECHR and Convention 108, which targeted not exclusively the protection of privacy, but privacy and more generally all individuals' rights and freedoms.[110] It suggested that the scope of the proposal should be rephrased, and not be limited to the right to privacy.[111]

In March 1992, the European Parliament adopted an Opinion[112] endorsing the draft Proposal, even if subject to a large number of changes (Heil 2010, p. 9). The Opinion included a proposed amendment to include in the preamble the assertions that 'automatic data-processing systems are designed to serve society', and that 'they must respect individual rights and freedoms, human identity and privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals'.[113] The European Parliament also submitted that the text should not apply to data 'contained in data files', but rather to 'the collection and processing of personal data'.[114] Many amendments advanced by the European Parliament reflected the perplexity initially generated in France by some clauses of the draft Proposal, such as, for instance, those foreseeing a different treatment for the public and the private sector.[115]

In February 1992 was signed the EU Treaty, known as the Treaty of Maastricht,[116] which entered into force on 1 November 1993. The Maastricht Treaty modified the

[108] Ibid. Recital 16.

[109] Opinion of the Economic and Social Committee (ESC) on the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks, and the proposal for a Council Decision in the field of information security [1991] OJ C159/38.

[110] Ibid. p. 40.

[111] Ibid.

[112] Opinion of the European Parliament on the Proposal for a Directive I COM(90) 0314– C3-0323/90– SYN 287: Proposal for a Council Directive concerning the protection of individuals in relation the processing of personal data (1st reading), adopted on 11 March 1992 [1992] OJ C94/173 (based on a report by Geoffrey Hoon).

[113] Opinion of the European Parliament… [1992] OJ C94/173, p. 175.

[114] Ibid.

[115] The report of Geoffrey Hoon was partially based on input by the French Mrs Fontaines and Vayssade (Brühann 1999, p. 15).

[116] Treaty on European Union, signed at Maastricht on 7 February 1992 (92/C 191/01) [1992] OJ C191/1.

procedure to be followed for the adoption of the legislative proposal, for which the European Parliament acquired co-decision competences.

In October 1992, the European Commission submitted a fully revised Proposal. The object of the Directive was no longer described as ensuring that Member States guarantee 'the protection of privacy of individuals in relation to the processing of personal data contained in data files', but, in words more consistent with Convention 108, ensuring that Member States guarantee 'the rights and freedoms of natural persons with respect to the processing of personal data, and in particular their right of privacy'.[117] The European Commission also incorporated into the revised text the idea put forward by the European Parliament according to which 'data-processing systems are designed to serve society', but chose to ignore its suggested allusion to the protection of human identity.[118] Additionally, the new proposal put an end to the distinction between the public and private sectors; consent was given more relevance; the notion of processing was introduced (displacing the notion of data file), and some exceptions and simplified procedures were incorporated for notification requirements (Guerrero Picó 2006, p. 62). Many of these changes were openly directed to mitigate French concerns (Brühann 1999, p. 15), with success, as France soon favoured the initiative.[119]

When the amended Proposal was discussed at the Council, Mediterranean countries and the Benelux were particularly supportive, whereas the UK and Ireland opposed the very idea of harmonising the field with a Directive. Germany appeared as undecided. It had trouble accepting the existence of a similar treatment for data processed in the private and the public sector, as well as with the notions of prior notification and sensitive data, and with the lack of provisions on internal data protection officers (issues contrasting with its own national modus operandi). Eventually, Germany joined the British, Irish and the also unconvinced Danish delegation to support a joint document against the Proposal (Brühann 1999, p. 16).

In the meantime, a White Paper on *Growth, competitiveness, employment* published by the European Commission following an initiative of its President, Jacques Delors, had stressed the need to protect 'privacy' as an element of the creation of an appropriate regulatory framework for the development of information networks (Commission of the European Communities 1993, p. 24). In response to the White Paper, the European Council requested in December 1993 to a group of 'prominent persons' chaired by the German Martin Bangemann[120] the preparation of a special report to identify measures to be taken into consideration in relation to Community backing of infrastructures and information. As a result, in May 1994 saw the light the *Europe and the global information society* report, also known as the Bangemann

[117] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (92/C 311/04), COM (92) 422 final—SYN 287, submitted by the Commission on 16 October 1992 [1992] OJ C311, p. 38.

[118] Ibid. p. 30.

[119] Referring to the fact that actually staff from the French Commission Nationale de l'Informatique et des Libertés (CNIL) had contributed to the new draft: (Pearce and Platten 1998, p. 533).

[120] At that time, Commissioner for the Internal Market and Industrial Affairs.

report (High Level Group on the Information Society (Bangemann Group) 1994, p. 5). The document devoted a whole section to privacy, and urged the Council to quickly come to a decision on the proposed Directive on data protection (1994, p. 22). In June 1994, the European Council formally invited 'the Council and the European Parliament to adopt before the end of the year measures in the areas already covered by existing proposals' in the area of information society.[121] Germany, which took over then the Presidency of the EU, managed to devise in collaboration with the European Commission a series of compromises allowing to obtain the support of the UK, such as special rules for the processing of data for medical research, and a transition period to apply the general norms to data processed manually (Brühann 1999, p. 17).[122]

The Council adopted a common position on the text in February 1995.[123] Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data[124] was finally approved on 24 October 1995.[125]

5.2.1.2 Object

Directive 95/46/EC does not formally endorse the notions of 'protection of personal data', or 'data protection'. As a matter of fact, its official title refers not to the protection of 'personal data' or even 'data', but to *the protection of individuals with regard to the processing of personal data.* Furthermore, the Directive describes one of its two main objectives as to oblige Member States to protect not 'personal data' or 'data', but rather the fundamental rights and freedoms of natural persons, and in particular their right to privacy (with respect to the processing of personal data).[126]

Contrary to Convention 108, which mentions 'data protection' in its Article 1, Directive 95/46/EC relegates the expression, together with 'personal

[121] Section 4 of Presidency Conclusions of European Council at Corfu, 24–25 June 1994.

[122] Noting the significance of this concession for the UK: (Carlin 1996, p. 65).

[123] Common Position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/…/EC of the European Parliament and of the Council of… on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/C 93/01) [1994] OJ C93/1.

[124] Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[125] The decision adopted by the European Parliament on such Common position included only a limited number of suggested amendments (Decision of the European Parliament on the common position established by the Council with a view to the adoption of a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (C4-0051/95– 00/0287 (COD)) (Co-decision procedure: second reading) [1994] OJ C166/105.

[126] Article 1(1) of Directive 95/46/EC.

data protection', to some marginal appearances in its text, concretely referring to 'personal data protection' officials,[127] sometimes designated as 'data protection' officials,[128] revealing the German roots of the notion of *Datenschutzbeauftragter,* that the English version adapted through a calque.[129] In reality, the German version of the Directive is comparatively extraordinarily inclined to use the word *Datenschutz* ('data protection'), even in instances where other languages merely refer to 'the protection of individuals'.[130] In any case, Directive 95/46/EC quickly came to be known, including in English-speaking circles, as the Data Protection Directive.

The object of Directive 95/46/EC is officially dual: it aims to ensure that Member States 'protect the fundamental rights and freedoms of natural persons, and in particular their right to *privacy*[131] with respect to the processing of personal data',[132] while at the same time forbidding any restrictions of the 'free flow of personal data between Member States'.[133]

The two elements of this dual purpose can be perceived as coming directly from Convention 108 (Dammann and Simitis 1997, p. 30), which referred to the protection of fundamental rights and freedoms, and in particular the right to privacy, in its Article 1,[134] and to the prohibition of restrictions to transborder data flows between parties in its Article 12. Their origins can be further traced back to the 1980 OECD Guidelines, the heading of which alludes to both 'the protection of privacy' and 'transborder flows of personal data', and which was conceptually shaped on the idea of reconciling competing demands. Actually, all international instruments try to balance both objectives (Rigaux 2002, p. 39), but, by mentioning both elements in its opening Article, Directive 95/46/EC reinforced the significance of each, as well as their configuration as rival values.

[127] Ibid. Article 18(2).

[128] Recitals 49 and 54, and Article 20(2) Directive 95/46/EC.

[129] Data protection is nevertheless also mentioned when describing a part of the contract between data controllers and data processors (Article 17(4) of Directive 95/46/EC).

[130] Recital 27 reads in its English version: 'Whereas the protection of individuals must…' (in French: '*considérant que la protection des personnes doit…*'; in Dutch: '*Overwegende dat de bescherming van personen…*'); cf. the German text: '*Datenschutz muß…*'.

[131] Emphasis added. This formulation is routenily repeated, except in Recital 34, which refers to the responsibility of Member States to protect 'the fundamental rights and the privacy of individuals'.

[132] Article 1(1) of Directive 95/46/EC.

[133] Ibid. Article 1(2).

[134] Article 1 of Convention 108: 'The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").'

5.2.1.3 Fundamental Rights and Freedoms, in Particular the Right to Privacy

The preamble to Directive 95/46/EC proclaims that 'the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to *privacy*,[135] which is recognised both in Article 8 of the (ECHR) and in the general principles of Community law'.[136] The Directive, in its English version, advances thus 'privacy' as a possible synonym for (respect for) 'private life', consistently with Convention 108, even if in contrast with the case law of the European Court of Human Rights (ECtHR) on Article 8 of the ECHR.

By 1995, the EU had eleven languages[137] recognised as equally binding and authentic. Of the eleven, only for two could be found guidance for terminological choices in the official versions of the ECHR and Convention 108: English and French, which are the official languages of the Council of Europe. Many other language versions followed expressions very close to the French, such as the Italian (with *vita privata*), the Portuguese (*vida privada*), or the Swedish (with *privatliv*), while the German version opted for the term *Privatsphäre* ('private sphere'). The Dutch text made use of the expression *persoonlijke levenssfeer* ('sphere of personal life'), echoing the Constitution of the Netherlands, whereas the Spanish text hesitated between *intimidad*, which reverberated the vocabulary of the Spanish Constitution and was mentioned among the Directive's objectives, and *vida privada*, preferred when referring to right protected by Article 8 of the ECHR.[138]

In the 1990s landscape of EC law, the prominence of the references to rights and freedoms in Directive 95/46/EC came across as an anomaly (Barnard and Deakin 2000, p. 343). Not only did it refer to the ECHR, but it even mentioned the Community commitment to the preservation and strengthening of peace and liberty and promoting democracy on the basis of the fundamental rights recognised in the constitution and laws of the Member States and in the ECHR.[139]

The European Court of Justice (ECJ) (currently integrated as an element of the Court of Justice of the EU) had already dealt by then with some cases related to the processing of data about individuals, even if hardly ever against the background of the protection of fundamental rights.[140] The Luxembourg Court had never, in any case, overtly connected the regulation of the processing of information about

[135] Emphasis added.

[136] Recital 10 of Directive 95/46/EC.

[137] Danish, Dutch, English, Finnish, French, German, Greek, Italian, Portuguese, Spanish, and Swedish.

[138] It appears also in the very provisions of the Directive: Articles 25(6) and 26(3) of Directive 95/46/EC.

[139] Recital 1 of Directive 95/46/EC.

[140] C-29/69 *Stauder v Stadt Ulm* [1969] ECR 419, Judgment of the Court of 12 November 1969. Cf. C-22/93 P *Campogrande v Commission* [1994] ECR I-1375, Judgment of the Court (Fifth Chamber) of 21 April 1994, on the communication by the Commission of the European Communities of the private address of officials to the Belgian authorities.

individuals to any right to privacy, to respect for private life, or to personal data protection.[141]

The adoption of Directive 95/46/EC soon had a major impact on the ECJ framing of the issue of data processing. This was already patent in 2000, in *Fisher*,[142] a judgment on the interpretation of a special provision of a 1992 Regulation[143] about databases containing information on arable fields, which obliged Member States to 'take the measures necessary to ensure protection of the data collected',[144] but failed to provide any details on what entailed such protection.[145] The Court was concretely required to clarify whether information provided by farmers could be transmitted to other farmers,[146] in spite of the obligation to ensure protection of the data. In its judgment, the Court interpreted the references in Directive 95/46/EC's preamble to the right to privacy as being part of the general principles of Community law[147] and to Convention 108[148] as jointly illustrating the fact that, even before the adoption of the Directive, its general principles already formed part of the general principles of Community law.[149]

Based on this assumption, the ECJ added that in order to apply the 1992 Regulation it was imperative for the competent authority to balance, on the one hand, the interest of the person who had provided the information, and, on the other, the interest of the person who wished to access it.[150] Moreover, the Court pointed out that such balancing needed to be assessed in a manner ensuring the protection of fundamental freedoms and rights,[151] for which Directive 95/46/EC (despite not having entered into force at the material time in the case in the main proceedings)[152] supplied suitable criteria.[153]

---

[141] Arguing in favour of an interpretation in which would transpire an implicit recognition: (Gutiérrez Castillo 2005, p. 17). See also: (Carlos Ruiz 2003, p. 15). In Case T-176/94 (T-176/94 *K v Commission* [1995] FP-I-A-0020 FP-II-00621, Judgment of the Court of First Instance (Third Chamber) of 13 July 1995) the applicant alleged that the disclosure of information about a dental problem was a violation of both his right to respect for private life under Article 8 of the ECHR and freedom of expression under Article 10 of the ECHR, but the Court of First instance dismissed his application.

[142] C-369/98 *Fisher* [2000] ECR I-6751, Judgment of the Court (Fourth Chamber) of 14 September 2000.

[143] Council Regulation (EEC) No 3508/92 of 27 November 1992 establishing an integrated administration and control system for certain Community aid schemes [1992] OJ L355/1.

[144] Article 9 of Regulation No 3508/92.

[145] *Fisher* § 25.

[146] Ibid. § 23.

[147] Recital 10 of Directive 95/46/EC.

[148] Ibid. Recital 11.

[149] *Fisher* § 34. Referring to this assertion as an isolated instance in ECJ case law: (Battista Petti 2006, p. 247).

[150] *Fisher* § 31.

[151] Ibid. § 32.

[152] Ibid. § 34.

[153] Ibid. § 33.

Subsequent case law underlined and reinforced the linkage between Directive 95/46/EC's provisions and Article 8 of the ECHR. In *Rundfunk*[154] (a case on the obligations of national authorities to disclose or not data about employees, and on the applicability of Community law in this context) the Luxembourg Court stressed that the clauses of the Directive 'in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to *privacy*,[155] must necessarily be interpreted in the light of fundamental rights' the observance of which is ensured by the Court as general principles of law.[156] The connection between the Directive's purposes and Article 8 of the ECHR was peculiarly manifest in the German original version of the *Rundfunk* judgment, which described Directive 95/46/EC as concerned with the *Achtung des Privatlebens*[157] (or 'respect for private life'), a terminology similar to the wording of Article 8 of the ECHR (on the right to respect for private) and different from the one de facto present in the German version of Directive 95/46/EC (which refers to the *Schutz der Privatsphäre*).[158]

In *Rundfunk*, the ECJ stressed that the fact that Directive 95/46/EC had been adopted using as legal basis an internal market provision did not mean that it was only applicable when were directly at stake internal market issues.[159] Observing that Article 8 of the ECHR establishes that in principle 'public authorities must not interfere with the right to respect for private life', but accepts some interferences,[160] the Court inferred that for the purpose of applying Directive 95/46/EC[161] 'it must be ascertained, first, whether legislation such as that at issue in the main proceedings provides for an interference with private life, and if so, whether that interference is justified from the point of view of Article 8' of the ECHR.[162] Then, the Court undertook such an assessments following the standard ECtHR procedure, and with direct references to Strasbourg's case law.[163] The judgment can ultimately be viewed as an attempt to read Directive 95/46/EC in the light of Article 8 ECHR (Oliver 2009, p. 1458) that, through a sort of 'cut and paste' integration of the case law of the

[154] Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, Judgment of the Court of 20 May 2003.

[155] Emphasis added.

[156] *Rundfunk* § 68.

[157] Ibid.

[158] This expression nevertheless also emerged in the judgment (see, for instance, § 53). In the English translation, these changes are echoed in appearances of both 'privacy' and 'private life'.

[159] *Rundfunk* § 41–42.

[160] Ibid. § 71.

[161] And in particular its Articles 6(1)(c), 7(c) and (e), and 13 (*Rundunk* § 72).

[162] Ibid. Advocate General Tizzano had also highlighted Article 8 of the ECHR as a relevant provision for the interpretation of Directive 95/46/EC in his Opinion for the Case. Nevertheless, he had also observed in a footnote that Article 8 of the ECHR had been 'repeated' in Article 7 of the Charter, and that Article 8 of the Charter referred specifically to the protection of personal data (Opinion of Advocate General Tizzano in C-465/00 *Rundfunk,* footnote 3).

[163] Inter alia, *Amann v* Switzerland [2000] RJD 2000-II, App. No 27798/95, and *Rotaru v. Romania* [2000] RJD 2000-V, App. No 28341/95, as well as *Leander v Sweden* [1987] Series A No 116, App. No 9248/81 (*Rundfunk* § 83).

ECtHR (Chalmers et al. 2006, p. 260), resulted in subordinating the applicability of Community legislation to an application of the ECHR (Sudre 2005, p. 410).[164]

Lindqvist[165] further consolidated the Court's seeming alignment of the interpretation of Directive 95/46/EC with Article 8 of the ECHR (Peers 2006, p. 509). The case had been triggered by the creation by a Swedish catechist of an Internet page displaying information about her colleagues in the parish, providing on some of them their full names, family circumstances, telephone numbers, and other details, including for instance that a particular person had injured her foot.[166] The Court of Justice was called upon to determine the applicability of Directive 95/46/EC, which it confirmed, and to provide guidance on the meaning of its provisions, which the Court declared should be interpreted taking into account the Directive's purposes of maintaining a balance between 'the protection of private life'[167] and freedom of movement of personal data.[168]

5.2.1.4 The Free Flow of Personal Data

Article 1(2) of Directive 95/46/EC identified as the instrument's second major objective to forbid any restrictions of the 'free flow of personal data between Member States',[169] thus substantiating its heading's allusion to the 'free movement' of personal data. These two expressions had their roots in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and in Convention 108, but acquired a whole new layer of meaning in the Directive, which placed them in the context of the creation of the internal market, seemingly construing the free flow of data as unhindered transfers of personal data among Member States, and thus close to Community principles of free movement.

The principles of the free movement of goods, persons, services and capital have always been contemplated as of crucial importance for Community law. They have been traditionally described as the EC *Grundfreiheiten* (Kingreen 2011, p. 515) (or 'fundamental freedoms')[170] by the German doctrine (Walter 2007, p. 17), and

[164] Also in this sense: (Korff 2004, p. 39). Commenting on *Rundfunk* as justifying constitutional concern: (De Hert and Gutwirth 2009).

[165] C-101/01 *Lindqvist* [2003] ECR I-12971, Judgment of the Court of 6 November 2003. See: (Coudray 2004).

[166] Opinion of AG Tizzano in Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] ECR I-12971.

[167] The English version of *Lindqvist* initially uses the word 'privacy' to refer to the provisions of Directive 95/46/EC (*Lindqvist* § 3 and 6), but, after mentioning that Article 8 of the ECHR provides for a right to respect for private life (§ 10), shifts to 'private life' (§ 86, 88, 97 and 99). The language of the case was Swedish, and the Swedish version invariably uses *privatliv(et)*.

[168] *Lindqvist* § 99.

[169] Article 1(2) of Directive 95/46/EC.

[170] Not to be confused with the 'fundamental freedoms' established by the ECHR.

eventually also by the ECJ.[171] The exact number of existing EC 'fundamental freedoms' has been debated, because, in addition to the well-established free movement of goods,[172] services,[173] capital,[174] and persons, can also be potentially identified, as different sub-categories, the free movement of workers[175] and the freedom of establishment.[176] These freedoms, envisaged as limiting both the action of the State and of supra-national institutions, have been advanced as the basis of the legitimacy of EC law and of its constitutional foundations (Poiares Maduro 1998, p. 166).

Adopting Directive 95/46/EC using as legal basis Article 100a of the EC Treaty, on the functioning of the internal market, called for the identification of a clear linkage between both. In this context, the preamble to the Directive recalls that, in accordance with Article 7a of the Treaty, the internal market requires the insurance of the free movement of goods, persons, services and capital,[177] and asserts that, as a result, it is necessary to ensure that personal data are able to flow freely from one Member State to another. It remains nevertheless unclear whether the free flow (or movement) of data serves the free movement of goods,[178] persons, services or capital.

Due to its support of the free flow of data, Directive 95/46/EC has been described as a tool of neutralisation of national rights in favour of economic efficiency (Thomas-Sertillanges and Quillatre 2011, p. 3). In reality, it corresponds to a wider trend in Community law, particularly developed during the 2000s, envisaging fundamental rights primarily as rights that can be invoked for the purpose of derogating from internal market freedoms.[179]

---

[171] C-55/94 *Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano* [1995] ECR I-04165, Judgment of the Court of 30 November 1995, § 37. The ECJ has also referred to these principles as 'fundamental' principles and 'foundations' of the EC Treaty. The free movement of workers has been dealt with as a fundamental right (C-152/82 *Forcheri v Belgian State* [1983] ECR 2323, Judgment of the Court (Fourth Chamber) of 13 July 1983, § 11), as has, indirectly, the free movement of goods (C-228/98 *Dounias* [2000] I-577, Judgment of the Court (Sixth Chamber) of 3 February 2000, § 64). See: (Szyszczak and Cygan 2008, p. 154).

[172] Articles 34 and 35 of the Treaty on the Functioning of the EU.

[173] Ibid. Article 56.

[174] Ibid. Article 63.

[175] Ibid. Article 45.

[176] Ibid. Article 49. See also: (Ehlers 2007, p. 176).

[177] Recital 3 of Directive 95/46/EC.

[178] In this sense: (Heil 2010, p. 31). The free movement of goods is primarily concerned with the free flow of products, which need not be tangible objects (Ehlers 2007, p. 176). They should be in principle be capable of constituting the object of commercial transactions, but this requirement is not strict (Epiney 2007, p. 277). Objects not falling under the category of goods could nevertheless be covered through the freedom of movement (Epiney 2007, p. 277).

[179] See, for instance: C-112/00 *Schmidberger* [2003] ECR I-5659, Judgment of the Court of 12 June 2003; and C-36/02 *Omega* [2004] ECR I-9609, Judgment of the Court (First Chamber) of 14 October 2004. See also: (Morijn 2006, p. 15).

5.2.2 Scope and Content

Directive 95/46/EC is presented by its preamble as containing 'principles of the protection of the rights and freedoms of individuals, notably the right to privacy' that 'give substance to and amplify those contained in' Convention 108.[180] Convention 108 is indeed one of its basic sources, together with national norms, as an outcome of the original will of the European Commission to combine different approaches existing in Europe,[181] and of the series of demands and compromises surfaced during the legislative process.

The references in the Directive's preamble to 'principles'[182] of the protection of the rights and freedoms of individuals allegedly set out by its provisions is somehow misleading. Contrary to other instruments, which effectively list principles,[183] Directive 95/46/EC does not explicitly devote any provisions to any principles, except when describing the '(p)rinciples relating to data quality'.[184]

Directive 95/46/EC applies to 'the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system'.[185] Thus, its scope goes beyond Convention 108, which covered only automated data processing (De Schutter 2003). 'Personal data' is defined as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[186] Compared to Convention 108, Directive 95/46/EC is more restrictive in the sense that it does not apply to data related to legal persons, which is a possibility explicitly left open in the Convention.[187]

Two major exemptions delimit the scope of application of Directive 95/46/EC. First, the Directive does not apply 'in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the

[180] Recital 11 of Directive 95/46/EC.

[181] In what was described as a comparative exercise (Brun 2002, p. 110).

[182] In addition to Recital 11, see also Recital 25 and 68 of Directive 95/46/EC.

[183] Notably, Convention 108, where Chapter II establishes the 'Basic principles for data protection', and the 1980 OECD Guidelines, which list a series of 'basic principles of national application' (in Part II).

[184] Which is the title of Section I, that as a matter of fact contains only one Article (Article 6).

[185] Article 3(1) of Directive 95/46/EC.

[186] Article 2(a) of Directive 95/46/EC.

[187] Article 3(2)(b) of Convention 108: Contracting States may inform the Council of Europe that they will also apply it to 'information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality'.

State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law'.[188] Second, the Directive shall neither apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity'.[189]

Directive 95/46/EC details applicable 'principles related to data quality', including that data must: be processed fairly and lawfully;[190] collected for specified, explicit and legitimate purposes and not further processed in incompatible ways;[191] adequate, relevant and not excessive in relation to the purposes of processing;[192] accurate and, where necessary, kept up to date;[193] and stored in a form permitting identification of data subjects only as long as necessary for the purposes of the processing.[194]

The Directive enumerates six criteria that can render data processing legitimate. The first one is that 'the data subject has unambiguously given his consent' to the processing.[195] The vision of consent as playing this noteworthy role came from Germany (Heil 2010, p. 10). In Convention 108, the only mention of consent referred to the need to obtain the express consent of the data subject when a designated authority wished to make requests for assistance.[196] Likewise, France also granted to consent a marginal role (Gentot 2000, p. 31).

Directive 95/46/EC establishes special norms for the processing of 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life', the processing of which is in principle prohibited,[197] and of data 'relating to offences, criminal convictions or security measures', to be accompanied by special safeguards.[198] The special treatment granted to some specific categories of data

[188] Article 3(2) of Directive 95/46/EC.

[189] Ibid. On this provision, see notably: (Wong and Savirimuthu 2008).

[190] Ibid. Article 6(1)(a).

[191] Article 6(1)(b) of Directive 95/46/EC, which also states that '(f)urther processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards'.

[192] Ibid. Article 6(1)(c).

[193] Ibid. Article 6(1)(d).

[194] Article 6(1)(e) of Directive 95/46/EC, which adds that 'Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use'.

[195] Ibid. Article 7(a). Other legitimate grounds include that processing is necessary for the performance of a contract to which the data subject is party (ibid. Article 7(b)); necessary for compliance with a legal obligation (ibid. Article 7(c)); necessary in order to protect the vital interests of the data subject (ibid. Article 7(d)); necessary for the performance of a task carried out in the public interest or in the exercise of official authority (ibid. Article 7(e)); or necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection (ibid. Article 7(f)).

[196] Article 15 of Convention 108.

[197] Article 8(1) of Directive 95/46/EC.

[198] Ibid. Article 8(5).

echoes related provisions in Convention 108,[199] and has traditionally played also a significant function in France and Ireland (Heil 2010, p. 10).[200]

A Section of the Directive[201] describes the 'Information to be given to the data subject', both when data are collected directly from the individuals concerned,[202] and in the other cases.[203] Individuals are recognised the right to access data[204] and a right to object to some data processing practices,[205] as well as a right not to be subject to some automated decisions[206] (a notion of French origin) (Church and Millard 2010, p. 82).[207] Directive 95/46/EC furthermore sets out obligations regarding the confidentiality and security of the processing,[208] and notification requirements.[209]

Member States are granted the possibility to restrict the scope of the rights and obligations established by the Directive if necessary to safeguard a series of aims such as national security, defence, public security; the prevention, investigation, detection and prosecution of crime; important economic or financial interests, and the protection of the data subject, or rights and freedoms of others.[210] These derogations were envisaged as corresponding to the same principles as those developed by the ECtHR in its case law on legitimate inferences by Article 8 of the ECHR (Kotschy 2010, p. 77). Moreover, some restrictions to the right of access are possible if for the purpose of scientific research.[211]

Directive 95/46/EC devotes a Chapter to the transfer of personal data to third countries. It establishes as basic premise that data transfers may take place only if the third country ensures an 'adequate level of protection',[212] but foresees also possible derogations,[213] or ways to enable transfers even in case of lack of 'adequate protection'. As it was apparent since the Directive's adoption that the US did not comply with the requirement of adequate protection, subsequent policy debates

[199] Although not exactly equivalent. On the differences, regarding both the types of data, and the special treatment granted, see: (Elías Baturones 1998, p. 1217).

[200] In contrast, it was less popular in Germany, where it was perceived as a special gesture towards those unconvinced by the necessity of data protection, but not contributing per se to the efficacy of the approach (see, in this sense: (Simitis 1985, p. 308)).

[201] Section IV.

[202] Article 10 of Directive 95/46/EC.

[203] Ibid. Article 11.

[204] Ibid. Article 12.

[205] Ibid. Article 14.

[206] Ibid. Article 15.

[207] In this sense, also: (Brun 2002, p. 110).

[208] Articles 16 and 17 of Directive 95/46/EC.

[209] Ibid. Articles 18–21. Observing that notification had an anchorage in French, British, and Scandinavian practice: (Heil 2010, p. 10).

[210] Article 13(1) of Directive 95/46/EC.

[211] Article 13(2) of Directive 95/46/EC. This clause reverberated a traditionally Danish approach to grant exceptions for scientific research (Heil (2010) op. cit. 10).

[212] Article 25 of Directive 95/46/EC. For critical assessments of the approach, see for instance: (Raab et al. 1999; Kuner 2009).

[213] Ibid. Article 26.

included many discussions on whether the US should bring its laws closer to the EU model, ignore Directive 95/46/EC as a non-tariff trade barrier, or search for an alternative solution (Westin 2003, p. 443). By the end of the 1990s, the Commission's services[214] and the US Department of Commerce started to work together with the view of adopting a set of arrangements allowing US companies to adhere to some data protection rules, known as the 'Safe harbor' principles.[215]

Moreover, Directive 95/46/EC foresaw the encouragement of the drawing up of codes of conduct intended to contribute to the proper implementation of data protection provisions.[216] This was of special interest for the Netherlands, customarily supportive of this type of instruments (Heil 2010, p. 10).

The Directive mandated that each Member State shall establish at least one independent supervisory authority to monitor the application of the implementing provisions,[217] an authority endowed with investigative powers, effective powers of intervention, and the power to engage in legal proceedings,[218] and responsible for hearing claims on the protection of rights and freedoms in regard to the processing of personal data.[219] It also set up, in its Article 29, what the English version of the Directive named a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, to have an advisory status, and composed of representatives of the supervisory authorities, as well as of a representative of the Commission.[220] The German version of the Directive designates the Working Party as the *Datenschutzgruppe*[221] ('data protection party'), but other language versions follow the English approach.[222] It eventually came to be known as the Article 29 Working Party.[223]

[214] The Internal Market and Services Directorate-General (DG MARKT), in close consultation with the Directorate-General for the External Relations (DG RELEX).

[215] Safe Harbor Privacy Principles, issued by the US Department of Commerce on 21 July 2000; Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour principles and related frequently asked questions issued by the US Department of Commerce (2006/520/EC) [2000] OJ L215/7. The adoption of this Commission Decision generated some tensions with the European Parliament, due to divergent interpretations on the applicability of the 'comitology' procedure followed by the Commission (see, for the Commission point of view: Corrigendum [2000] OJ L115/14). See also: (Regan 2003; Dhont et al. 2004; Busch 2006).

[216] Article 27 of Directive 95/46/EC.

[217] Article 28(1) of Directive 95/46/EC.

[218] Ibid. Article 28(3).

[219] Ibid. Article 28(4).

[220] Ibid. Articles 29 and 30.

[221] See heading of Article 29 of Directive 95/46/EC.

[222] In the French version: *Groupe de protection des personnes à l'égard du traitement des données à caractère personnel.* Dutch version: *Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens*.

[223] On this Working Party, see, notably: (Poullet and Gutwirth 2008).

5.2.3 Directive 97/66/EC

The European Commission had introduced in its 1990 Communication a proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks, to supplement the 'general directive'.[224] The Commission observed then that the Council[225] and the European Parliament[226] had both stressed the importance of appropriate measures being taken in this field, and that data protection authorities were equally concerned.[227]

The original draft of the proposal presented in 1990 identified as its main object 'to ensure an equal level of *protection of privacy*[228] in the Community and to provide for the free movement of telecommunications equipment and services within and between Member States'.[229] In 1994, the European Commission presented a second draft,[230] which described its object as to provide 'an equal level of *protection of personal data and privacy*'.[231,232]

---

[224] COM(90) 314 final, p. 8.

[225] The 1990 Communication of the Commission refers notably to Council Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (88/C 257/01) [1988] OJ C257/1), where there is only an incidental allusion to the need 'to see that workers have the right skills to protect personal data' (ibid. 2); and to Council Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (89/C 196/04) [1988] OJ C196/4), where can be found a call to further discussion 'regarding user privacy protection requirements' in the context of features of new services (ibid. p. 5).

[226] The 1990 Communication of the Commission mentions the Resolution of the European Parliament closing the procedure for consultation of the European Parliament on the proposal from the Commission of the European Communities to the Council for a Recommendation on the coordinated introduction of the Integrated Services Digital Network (ISDN) in the European Community of 12 December 1986, Doc. A2-178/86 [1987] OJ C 7/334, which alludes to ensuring, within the emerging ISDN, 'a consistent level of data privacy protection' (ibid. p. 335); and a Resolution of the European Parliament on posts and telecommunications (Doc. A 2-259/88) of 14 December 1988 [1989] OJ C12/69, calling upon the Commission to propose 'measures to ensure data privacy protection and confidentiality' (ibid. p. 71), and reminding the Commission of its responsibility to accompany legislative proposals on opening telecommunications markets 'by action at Community level relating to the protection of personal data' (ibid.).

[227] COM(90) 314 final, p. 7.

[228] Emphasis added.

[229] SYN 288.

[230] Commission of the European Communities, *Amended proposal for a European Parliament and Council Directive concerning the protection of personal data and privacy in the context of digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and digital mobile networks (presented by the Commission pursuant to Article 189a(2) of the EC Treaty)*, COM(94) 128 final—COD 288, Brussels, 13.06.1994, p. 11.

[231] Emphasis added.

[232] COM(94) 128 final, p. 11.

The word privacy was by the mid-1990s used in Community law not only in relation to the protection of personal data (as, for instance, in Directive 95/46/EC). It was also used in the field of electronic communications. And, as in Directive 95/46/EC, the term privacy was in this field sometimes connected to Article 8 of the ECHR. In this sense, in 1997 was adopted Directive 97/7/EC on the protection of consumers in respect of distance contracts,[233] which, explicitly referencing Article 8 of the ECHR, hinted that shall be recognised a 'consumer's right to privacy',[234] protecting consumers against particularly intrusive means of communication.[235] From this standpoint, Directive 97/7/EC set out restrictions on the use of certain means of distance communication, and required the prior consent of the consumer for the use of automated calling systems without human intervention and fax as a means of distance communication for the conclusion of contracts.[236]

Directive 97/66/EC, concerning the processing of personal data and the protection of privacy in the telecommunications sector,[237] rooted in the 1990 draft Proposal, was finally adopted in December 1997. It defines its object as 'to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community'.[238] There were thus two main changes incorporated to the 1990 draft Proposal's definition of its object in order to increase consistency with Directive 95/46/EC: first, a reference to the protection of fundamental rights and freedoms in general; second, the mention of the 'free movement' of personal data.

Directive 97/66/EC was formally envisaged as a *lex specialis* developing for a concrete sector (the telecommunications sector) the more general rules of Directive 95/46/EC. It did not, however, limit itself to that purpose. Its scope is defined by stating that its provisions both 'particularise and complement Directive 95/46/EC'.[239] The way in which Directive 97/66/EC complements Directive 95/46/EC[240] is seemingly primarily by integrating provisions destined to protect aspects of the rights enshrined in Article 8 of the ECHR that cannot be subsumed in issues related

[233] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts [1997] OJ L144/19. See also: (Asscher and Hoogcarspel 2006, p. 20).

[234] On this notion, see notably: (Cavanillas Múgica 2008).

[235] Recital (17) of Directive 97/7/EC.

[236] Ibid. Article 10(1).

[237] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1997] OJ L24/1.

[238] Article 1(1) of Directive 97/66/EC.

[239] Ibid. Article 2.

[240] According to some, in a way that considerably enlarged its scope (Büllesbach et al. 2010, p. 4).

to the processing of personal data—for instance, it overtly touches upon the issue of the confidentiality of communications.[241]

Directive 97/66/EC, nonetheless, fails to deliver a clear picture of to what extent it particularises Community protection of personal data, and to what extent it complements it. It is also vague in the identification of the rights at stake, and the exact meaning it attributes to the word 'privacy'. The English version of Directive 97/66/EC refers to privacy in its heading, but occasionally it also uses the expression 'private life',[242] as well as the word 'confidentiality', in particular when referring to the '(c)onfidentiality of the communications'.[243] The German version generally uses *Privatsphäre*,[244] opting for *Vertraulichkeit* as equivalent to 'confidentiality', but sometimes also as equivalent of privacy.[245]

An interesting peculiarity surfaces in the Portuguese version. While the Portuguese version of Directive 95/46/EC describes as one of its objectives the protection of, in particular, the *vida privada* of individuals, Directive 97/66/EC is advanced as concerned with ensuring in the telecommunications sector the protection of personal data and of *privacidade*.[246] This opens the question of whether the meaning of the different instances of the English 'privacy' in the two instruments shall be regarded as coincidental, taking into account that they have been translated differently.

Directive 97/66/EC actually introduced a notion that appeared to be at the crossroads of personal data protection and the confidentiality of communications: 'traffic data',[247] described as data processed to establish calls, but that according to the Directive's provisions shall in principle be erased or made anonymous upon the call's termination. The roots of this notion could be traced back to the 1984 *Malone* judgment[248] of the ECtHR, which placed communications' data under the light of the right to confidentiality of communications.[249]

Directive 97/66/EC contained provisions similar to those that Directive 97/7/EC had framed under the 'consumer's right to privacy', to be applied to unsolicited calls and faxes. With the aim of providing safeguards for all subscribers of

[241] Another example of the way in which Directive 97/66/EC seemingly went beyond Directive 95/46/EC is its mention of the legitimate interests of legal persons (Article 1(2) of Directive 97/66/EC). See: (Martínez Martínez 2004, p. 227).

[242] Recital (17) of Directive 97/66/EC notes: 'data relating to subscribers processed to establish calls contain information on the private life of natural persons'.

[243] Article 5 of Directive 97/66/EC.

[244] The German version is titled *Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation*. However, it uses the word *Privatleben* in Recital 17.

[245] In Recital 19, on 'privacy options' for telephone services.

[246] The title of the Portuguese version is *Directiva 97/66/Ce do Parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações*. The Portuguese version refers to *vida privada* only in Recital 17.

[247] Article 6 of Directive 97/66/EC.

[248] *Malone v the United Kingdom* [1984] Series A No 82, App. No 8691/79.

[249] Ibid § 84. See also: (Frígols i Brines 2010, p. 48).

telecommunication services against intrusion into their 'privacy' by means of unsolicited calls and faxes,[250] Article 12 of Directive 97/66/EC established an opt-in regime for the use of any automated calling machines without human intervention, including faxes, for purposes of direct marketing. These clauses eventually led to others explicitly referring to unsolicited communications through electronic mail (Asscher and Hoogcarspel 2006, p. 23), introduced however not in legal instruments directly dealing with the protection of personal data, but in Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce').[251] Additionally, Directive 97/66/EC made an explicit reference to the 'right to privacy' of individuals making and receiving telephone calls, a right to privacy which can presumably be affected by the elaboration of itemised telephone bills (thus, the Directive granted a right to non-itemised bills).[252]

5.2.4 Data Protection and EC Institutions and Bodies

Directive 95/46/EC being a Directive, it mandates Member States to adopt provisions transposing its content, but it does not directly bind the Community institutions and bodies. The Commission was aware of this, and it had accompanied its 1990 draft Proposal with a declaration on the fact that Community institutions shall apply the same data protection principles as those developed in the Directive.

5.2.4.1 Article 286 of the EC Treaty

Two years after the adoption of Directive 95/46/EC, in 1997, was signed the Treaty of Amsterdam,[253] which entered into force on 1 May 1999. The Amsterdam Treaty brought about substantial changes. It incorporated in the Treaty establishing the European Community (EC Treaty) a new provision, Article 286, establishing that from January 1999 'Community acts on the protection of individuals with regard to the processing of personal data *and the free movement of such data*[254] shall apply to the institutions and bodies' set up by, or on the basis of, the EC Treaty.[255]

[250] Recital (22) of Directive 97/66/EC.

[251] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L78/1 (see Article 7). See also: (Asscher and Hoogcarspel 2006, p. 21).

[252] Article 7 of Directive 97/66/EC.

[253] Signed on 2 October 1997. Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts (97/C 340/01) [1997] OJ C340/1.

[254] Emphasis added.

[255] Article 286(1) of the EC Treaty.

Article 286 of the EC Treaty appeared to bring about still a new (and vague) construe of the idea of the 'free movement' of personal data. Whereas Directive 95/46/EC seemed to portray the notion of 'free movement' as an element of the internal market (forbidding obstacles to free movement of data among Member States), in the context of Article 286 what was at stake was the processing of personal data by Community institutions, and thus the exact meaning of the unhindered flows of data among EC institutions and bodies, a 'free movement' that through Article 286 of the EC Treaty was granted Treaty-level recognition, was unclear.

Article 286 of the EC Treaty also specified that, from January 1999, shall be put in place a new independent supervisory body responsible for the monitoring of relevant provisions applicable to EC institutions and bodies. The European Commission was reputedly initially reticent to such idea, concerned with a possible overlap with the European Ombudsman (Oreja Aguirre and Fonseca Morillo 1998, p. 425).

5.2.4.2 Regulation (EC) No 45/2001

To implement the obligations laid down in Article 286 of the EC Treaty, in 1999 the European Commission adopted a proposal for a Regulation on the protection of individuals with regard to the processing of personal data by Community institutions and bodies, and on the free movement of such data,[256] leading to the adoption on 18 December 2000 of Regulation (EC) No 45/2001.[257] The Regulation's scope of application covers all the processing of personal data by Community institutions and bodies insofar as it is carried out in the exercise of activities falling within the scope of Community law.[258]

Regulation (EC) No 45/2001 describes its object by establishing that Community institutions and bodies shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, and 'shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC'.[259] This reference to the free flow of personal data was absent from the original 1999 Proposal by the Commission.[260] The sentence links the idea of a 'free flow' of personal data to data transfers among

[256] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (1999/C 376 E/04) (Text with EEA relevance) COM(1999) 337 final—1999/0153(COD) (Submitted by the Commission on 17 September 1999) [1999] OJ C376/24.

[257] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1.

[258] Article 3(1) of Regulation (EC) No 45/2001.

[259] Ibid. Article 1(1).

[260] COM(1999) 337 final, p. 25.

Community institutions and bodies, but also between them and any parties subject to Directive 95/46/EC.

Article 2 of Regulation (EC) No 45/2001 entrusts the new independent supervisory authority, named European Data Protection Supervisor (EDPS),[261] with the monitoring of the application of the Regulation's provisions.[262]

5.2.5 Third Pillar Data Protection

The legislative package presented in 1990 by the European Commission included a text that failed to generate any support in the Council: a Draft resolution of the representatives of the Member States of the European Communities designed to extend its principles to processing activities not governed by Community law.[263] This lack of enthusiasm heralded long discussions on the possible opportunity of adopting general 'data protection' instruments to what was to be known during more than 15 years 'the third pillar'.

Between 1993[264] and 2009,[265] the EU was divided into three pillars. The first pillar corresponded to the European Communities. The second pillar coincided with the Common Foreign and Security Policy (CFSP).[266] The third pillar, in its original formulation, covered issues ranging from asylum and immigration to police and judicial cooperation in criminal matters (Craig and De Búrca 2011, p. 924). In 1997, the Treaty of Amsterdam created an Area of Freedom, Security and Justice (AFSJ),[267] and moved out of the third pillar, and into the first one, a series of matters such as visas, immigration and asylum (Peers 2006, p. 130). The Amsterdam Treaty also launched the incorporation into EU law of the Schengen Convention.[268]

Directive 95/46/EC applied to data processing in the course of first pillar activities, but not to those falling under the third pillar.[269] Different third pillar legal instruments requiring the processing of data about individuals integrated their own 'data protection' norms, as it had already been the case with the 1990 Schengen

[261] See, notably: (Hijmans 2006).

[262] See Chapter V of Regulation (EC) No 45/2001.

[263] COM(90) 314 final, p. 7.

[264] The pillar structure was introduced by the Treaty of Maastricht on 1 November 1993.

[265] The pillar structure collapsed on 1 December 2009 with the entry into force of the Treaty of Lisbon.

[266] Governed by Title V of the EU Treaty after the entry into force of the Maastricht Treaty.

[267] See, on its early years: (Walker 2004).

[268] The Schengen acquis—Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L239/19.

[269] Because of its legal basis, and as confirmed in Article 3(2) of Directive 95/46/EC.

Convention. The same approach was followed, notably, in relation with Europol,[270] formally established as a European Police Office by the Convention of 26 July 1995,[271] which entered into force on 1 October 1998. The preamble to the 1995 Europol Convention stated that in the field of police co-operation particular attention must be paid to the protection of the rights of individuals, and notably the protection of their personal data. Europol Convention's provisions repeatedly refer to Convention 108.[272]

In 1997, the Amsterdam Treaty noted that in the context of Europol should be promoted common action in the field of police cooperation including 'the collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions, in particular through Europol, subject to appropriate provisions on the *protection of personal data'*.[273] The Europol agency itself, based in Den Hague, is operational since July 1999 (Delarue 2010, p. 145).[274]

Typically, third pillar instruments adopted during this period conditioned access to data processed in their context to the insurance by Member States of a level of protection of personal data at least equal to that resulting from the principles of Convention 108, taking also into account Recommendation No R(87)15 of 17 September 1987[275] of the Committee of Ministers of the Council of Europe.[276]

[270] Europol was first mentioned by the Maastricht Treaty of 1992 as a Union-wide system for exchanging police information in relation to the fight against terrorism, drug trafficking and other international crime. The idea of its creation was first launched in 1991 (Delarue 2010, p. 145). On Europol and data protection, see also: (Esquinas Valverde 2010).

[271] Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) [1995] OJ C316/2.

[272] See, for instance: Article 10(1)(2) ('Collection, processing and utilisation of personal data').

[273] Article 30 of Treaty of Amsterdam.

[274] Europol is now regulated by a Council Decision adopted on 6 April 2009, which became applicable on 1 January 2010 (Council Decision of 6 April 2009 establishing the European Police Office (Europol) [2009] OJ L121/37). See also: (Piris 2010, p. 182).

[275] Recommendation No R(87)15 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, adopted on 17 September 1987. On this Recommendation, see notably: (Boehm 2012, p. 96 ff.).

[276] See, notably: Council Act 95/C316/02 of 26 July 1995 drawing up the Convention on the use of information technology for customs purposes [1995] OJ C316/33. See also: Council Act 98/C 24/01 of 18 December 1997 drawing up, on the basis of Article K3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations [1998] OJ C24/1; it establishes in its Article 25(1) (Data protection for the exchange of data): 'When information is exchanged, the customs administrations shall take into account in each specific case the requirements for the protection of personal data. They shall respect the relevant provisions of the Convention of the Council of Europe of 28 January1981 for the protection of individuals with regard to automatic processing of personal data'.

5.3 Impact on National Laws

EU involvement in the regulation of data processing contributed to the reinforcement of the significance of Convention 108 across Europe, and simultaneously promoted the norms established by its own legal system. The year 1995 was in this sense crucial, as it marked both the coming into existence of the Schengen Area,[277] and the adoption of Directive 95/46/EC. It can thus be regarded as initiating a new phase of development of national norms in Europe (Simitis 2006). The impact was however not immediately perceptible in all countries.

Directive 95/46/EC granted Member States 3 years to adapt their national legislation to its content.[278] At the time of its adoption, two Member States still had no special laws on the protection of personal data (namely, Italy and Greece) (Heil 2010, p. 10), and the others had to bring their legislation in line with the Directive's requirements. Transposition into national laws was slower than expected by the European Commission. In 1999, the Commission initiated proceedings against a number of Member States[279] for failure to notify all the necessary measures to implement the Directive.[280] The Commission officially had to issue a report to the Council and the European Parliament on the Directive's implementation no later than 3 years after its entry into force,[281] but at the end of 2001[282] the responsible Commissioner[283] announced that the report would be delayed due to the slow pace of transposition by Member States (European Commission 2003, p. 1).

5.3.1 Already Acceded EU Member States

Italy was seemingly one of the first Member States to react to the adoption of Directive 95/46/EC, which it transposed by an Act adopted in 1996.[284] The truth is, however, that Italy had signed Convention 108 in 1983, and that it had prepared already then a legislative proposal on data protection, but during many years had failed to achieve the approval of any Act on this issue. The adoption in 1996 of the

[277] After the signature by Portugal and Spain.

[278] Directive 95/46/EC was incorporated in 1999 into the 1992 *Agreement on the European Economic Area* (EEA), and States which are not members of the EU but party to the EEA Agreement (ie, Norway, Iceland and Liechtenstein) are also legally bound to bring their respective laws into conformity with the Directive.

[279] France, Germany, Ireland, Luxembourg and the Netherlands.

[280] European Commission, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States: Technical Annex* 1 (2003).

[281] Article 33 of Directive 95/46/EC.

[282] The Internal Market Council of 26 November 2001.

[283] Commissioner Frits Bolkestein.

[284] There were however some punctual provisions dealing with related issues, such as a few clauses in a 1970 statute, limiting the surveillance of workers (Frosini 1982, p. 26).

Legge 31 dicembre 1996, n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*[285] ('Protection of persons and other subjects relating to the processing of personal data') finally allowed Italy to ratify Convention 108, as well as to enter the Schengen Area, and to comply with Directive 95/46/EC (Rodotà 2005, p. 31).

The 1996 Italian Act inscribed in Italian positive law the existence of a right to *riservatezza,* as well as a right to personal identity (*all'identita' personale*). The Act's object was described as guaranteeing that personal data processing occurs in compliance with rights and fundamental freedoms, but also in accordance with the dignity of natural persons, notably in relation with their *riservatezza* and personal identity.[286] The right to *riservatezza* was mentioned in the 1996 Act in place of the references of the Italian version of Directive 95/46/EC to the right to *vita privata*;[287] consequently, in a sense the Italian Act translated EC's Italian *vita privata* as *riservatezza*.

Before 1996, only the judiciary had acknowledged the existence of a right to *riservatezza* in Italy (Niger 2006, p. 53).[288] Its judicial creation had experienced different stages, moving from a linkage with Article 8 of the ECHR to an anchorage in Article 2 of the Italian Constitution, which states that the Italian Republic recognises and ensures the inviolable rights of individuals both as single individuals and in the social relations where their personality evolves.[289] The Italian right to personal identity was also originally created by the judiciary, starting in the mid-1970s. Surfaced in connection with the right to a name and the right to image, Italy's right to personal identity has been defined as the interest of individuals not to see altered their own intellectual, political, social, religious or professional condition because of an attribution of ideas, opinions, or behaviours different than those considered as own by the individual himself (Pino 2006, p. 257). The 1996 law, by identifying *riservatezza* and personal identity as its ratio, positively placed these rights in the horizon of Italian fundamental rights (Pino 2006, p. 257).[290]

In addition, the 1996 Act also marked the adoption by the Italian language of the English word *privacy*.[291] The term was absent from the Act itself, which was

[285] See: (Cuffaro and Ricciuto 1997).

[286] Article 1(1) of *Legge N° 675* of 1996*: 'La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle liberta' fondamentali, nonche' della dignita' delle persone fisiche, con particolare riferimento alla riservatezza e all'identita' personale; garantisce altresi' i diritti delle persone giuridiche e di ogni altro ente o associazione'*. Describing the wording as an enhanced rewriting of Directive 95/46/EC: (Rodotà 2005, p. 31).

[287] Article 1(1) of Directive 95/46/EC.

[288] On this right, see also: (Riolfo Marengo 1993, p. 1054).

[289] Article 2 of Italian Constitution: '*i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità'*. See: (Niger 2006, p. 1054). See also: (Rigaux 1990, p. 150). On the elasticity of Article 2 of the Italian Constitution: (Solinas 2011, p. 147).

[290] Some consider this moment as the culmination of a long path towards the construction of the rights of personality in Italy: (Ricciuto 2011, p. 40).

[291] Noting the linkage between the usage of the word *privacy* in Italian and the regulation of data processing: (Serrano Pérez 2003, p. 37).

however often referred by commentators as the *legge sulla privacy* (Pino 2002, p. 135). The usage of the word privacy has ever since been varied: sometimes it is used as synonymous with the right to *riservatezza*, or with the expression right *alla intimità della vita privata*, but, generally, it has been described as having incorporated into Italian language an added source of semantic ambiguity (Pino 2002, p. 135), illustrated by the historical coexistence of a number of concomitant idioms and terms, including the synthetic *privatezza* (Niger 2006, p. 39).

Greece ratified Convention 108 in 1992, but did not adopt any national instrument regulating data processing until 1997, when Law No. 2472 on the Protection of Individuals with Regard to the Processing of Personal Data[292] transposed Directive 95/46/EC into Greek law.

Sweden had its pioneering *Datalag* since 1973. Already in June 1995, before the formal adoption of Directive 95/46/EC, the Swedish government entrusted a committee with the task of studying necessary amendments to the *Datalag* (Magnusson-Sjoberg 1999, p. 38)—which included the possible need to widen the scope of application to cover not only automated processing, but also manual processing (Seipel 1996). In 1998, a new Personal Data Act[293] transposed Directive 95/46/EC. The new Act consolidated the traditional Swedish framing of the issue in terms of protecting individuals against the violation of their personal integrity by processing of personal data (Bygrave 2002, p. 37).

In the UK, some were concerned that the allusions to privacy in Directive 95/46/EC might oblige the transposing national act to similarly incorporate explicit references to 'privacy', which was not recognised as a right in the UK legal system (Chalton 1997, p. 27). Eventually, the UK adopted in 1998 a Data Protection Act[294] that, exactly as the 1984 act it replaced, does not refer to privacy. In 1998, however, received Royal assent the Human Rights Act 1998, which obliges UK courts and public bodies to apply the rights set out in the ECHR, including Article 8 of the ECHR on the right to respect for private life, generally perceived as a key step for the protection of privacy in the UK (O' Cinneide et al. 2006, p. 555). The Data Protection Act was thus soon presented as needing to be interpreted in this particular light (Critchell-Ward and Landsborough-McDonald 2007, p. 528). The way in which personal data protection and privacy were eventually connected in the implementation of the 1998 Data Protection Act led, however, to some frictions with the European Commission, concerned that privacy was being used to mould restrictively the scope of application of the transposing instrument (Chalton 2004, p. 179). Such restrictive reading of the scope of application was based concretely on a restrictive reading of the notion of 'personal data' (Kranenborg 2008, p. 1107), which understands the adjective 'personal' as related to 'private' in the sense of

[292] In April 1997.

[293] Personal Data Act (*personuppgiftslagen*) (1998:204), issued on 29 April 1998. It came into force on 24 October 1998.

[294] Passed on 16 July 1998, and entered into force on 1 March 2000, after the issuing of first subsidiary regulations. The Act contains eight principles applicable to the processing of personal data.

non-public.[295] This reading can be partially explained by the influence of the notion of 'private information' sustained in the context of the development of modern UK approach to privacy.[296]

The first European country to incorporate provisions on the regulation of data processing into its Constitution, Portugal, had adopted in 1991 the *Lei da Protecção de Dados Pessoais face à Informática*, or Law on the Protection of Data vis-à-vis Computers,[297] mandating that automated data processing shall be transparent and respect the private and family life, and the fundamental rights, freedoms and safeguards of citizens.[298] The primary objective was then to prepare Portugal for the signature of the Schengen Agreement in 1995. The 1991 Law was reviewed in 1998, with the passing of the *Lei da Protecção de Dados Pessoais* (no longer referring in its heading to computers),[299] that transposed Directive 95/46/EC. In full accordance with the Portuguese version of the Directive, it alluded to the need to respect the *vida privada* (private life) of individuals, but not in conjunction with family life as it had been the case in the 1991 Law.[300]

Belgium had since 1992 a specific Law, which was modified in 1998[301] to implement Directive 95/46/EC. Whereas in 1992 the legislator had followed the approach according to which personal data processing is in principle generally authorised (except for 'sensitive data'), in 1998 was integrated the Directive's perspective, pursuant to which data processing is generally not authorised, except on a series of (broadly) enumerated grounds (F. De Brouwer 1999, p. 183). In 1994, Belgium had integrated into its Constitution a provision enshrining the right to *vie privée* (in the French version), or *privé-leven* (in the Dutch version). The modified 1992 Law, however, kept in its Dutch version the original references to the protection of the *persoonlijke levensfeer*, in accordance with the Dutch version of Directive 95/46/EC.

---

[295] This trend appears also in the literature. See, for instance: (Wacks 1989, p. 26), where the following definition of 'personal information' is proposed: ''Personal information' consists of those facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore want to withhold or at least to restrict their collection'.

[296] See, notably: *Douglas v Hello!* ([2001] QB 967; *McKennitt v Ash* [2008] QB 73[11]). See also: (Moreham 2001, p. 767).

[297] *Lei n.º 10/91 de 29 de Abril.*

[298] Article 1 of Law 10/91: *'O uso da informática deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais do cidadão'.*

[299] *Lei n.º 67/98 de 26 de Outubro.*

[300] Article 2 of Law 67/98: 'O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais'.

[301] *Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens, 8 december 1998.* See, notably: (Thierry and Poullet 1999).

In 1992, Spain[302] had adopted the first legal instrument giving substance to the mandate to legislate of Article 18(4) of the Spanish Constitution,[303] mainly to allow Spain to enter the Schengen Area, and drafted already taking into account the proposal of the European Commission that eventually became Directive 95/46/EC (Murillo de la Cueva 2009, p. 21): the *Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal* (LORTAD),[304] or Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data. The preamble of this 1992 Law placed its provisions in the context of the protection of the *privacidad* of individuals, explicitly distinguishing this word from the term *intimidad*, and arguing that whereas *intimidad* was concerned with the sphere in which are developed the most reserved dimensions of a person's life, *privacidad* referred to a wider spectrum of dimensions, facets that were possibly irrelevant separately, but that together draw up a picture of the individuals' personality that they are entitled to be kept concealed.[305] The term *privacidad*, derived from the English privacy, was a neologism.[306]

In 1995, a new Spanish Criminal Code threw some ambiguity on the meaning of these notions, by placing under a heading mentioning the protection of the *intimidad* of individuals a provision against the misuse of *datos reservados de carácter personal* ('confidential personal data'), an unprecedented category of data (Anarte Borrallo 2003, p. 225).[307]

Spain implemented Directive 95/46/EC in 1999, with the *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD).[308] The 1999 legislator avoided dealing with the issue of the constitutional framing of

[302] Which had ratified Convention 108 in 1984.

[303] Since 1982, Spain had the *Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen* (BOE núm. 115 de 15 de mayo de 1982), which included a transitory provision stating that, while there was no instrument developing the mandate of Article 18(4) of the Spanish Constitution, the civil protection of '*honor y la intimidad personal y familiar'* against unlawful interferences derived from the use of computers were to be regulated by its provisions (Lesmes Serrano 2008, p. 48).

[304] *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) (BOE núm. 262 de 31 de octubre de 1992).*

[305] Paragraph 1 of preamble to the LORTAD. This distinction was not sustained in the following paragraphs of the preamble, which went on to advocate the need to delimit new boundaries for *intimidad* (and honour) to protect them in the face of automated data processing, claiming that the purpose of Article 18(4) of the Constitution was to fix such a boundary. Nonetheless, its discussion illustrated a will to move beyond pre-computers conceptions of privacy (Martínez Martínez 2004, p. 18).

[306] Until then, the doctrine had generally tended to refer to the content of Article 18(4) of the Spanish Constitution in terms echoing the French *informatique et libertés*, such as *libertad informática* ('computer freedom').

[307] See also: (Gómez Navajas 2005, p. 82).

[308] BOE núm. 298 de 14 de diciembre de 1999. Some provisions of the 1999 LOPD were the object of a constitutional challenge promoted by the Spanish ombudsman, the Defensor del Pueblo, resolved in the emblematic *Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre*. See, notably: (Abad Amoros 2013). See also Chap. 6, Sect. 6.2.1, of this book.

personal data protection: contrary to the 1992 LORTAD, the 1999 LOPD lacked a preamble (Murillo de la Cueva 2009, p. 23). Its purpose was defined in terms very similar to those of Directive 95/46/EC, but combined with additional words coming from the Spanish Constitution, resulting in the assertion that it served, in relation with personal data processing, the fundamental rights and public freedoms[309] of natural persons, and especially their honour and *intimidad personal y familiar*[310].[311]

Also in 1999, Finland revised its personal data protection legislation, which dated back to 1987. The 1999 *Henkilötietolaki*[312] (Personal Data Act)[313] transposed Directive 95/46/EC, and aimed also at accommodating the Finnish constitutional reform of 1999.[314] The 1999 Finnish Act advances as its objectives to implement, in the processing of personal data, the protection of *yksityiselämän*[315] (translatable as 'private life') and other basic rights safeguarding the right to *yksityisyyden*[316] (translatable as 'privacy'), as well as to promote the development of and compliance with good processing practice.[317] According to the 1999 Personal Data Act, thus, the protection of private life served the protection of privacy, which has been interpreted as exemplifying the marked instability of the framing of these notions in Finnish law (Saarenpää 2008, p. 23). Regardless of what the Personal Data Act might appear to hint, the protection of private life is a fundamental right recognised by the Finnish Constitution, while privacy (sometimes referred as 'personal integrity') is a concept used primarily by the Finnish Criminal Code (Saarenpää 2008, pp. 22–23).

Austria, which had a Data Protection Act since 1978, revised it in 2000 with the *Datenschutzgesetz* (DSG) 2000, or Data Protection Act of 2000.[318] Just as the previous Act, this Act recognised a fundamental right to data protection (*Grundrecht auf Datenschutz)*,[319] defined as a right to the secrecy of personal data, especially with regard to private and family life, insofar as individuals have an interest deserving such protection.[320]

---

[309] Cf. Article 1 of the Spanish version of Directive 95/46/EC, not qualifying freedoms as 'public freedoms'.

[310] Cf. Article 1 of the Spanish version of Directive 95/46/EC, referring just to the particular protection of the '*derecho a la intimidad'*.

[311] Article 1 LOPD. Underlining the absence of any reference to Article 18(4) of the Spanish Constitution: (Murillo de la Cueva 2009, p. 23).

[312] *Personuppgiftslag* in the Swedish version.

[313] Act 523/1999.

[314] Constitution of Finland (731/1999).

[315] *Privatlivet* in the Swedish version.

[316] *Personliga integriteten* in the Swedish version.

[317] Section 1 of Chapter 1 of 1998 Personal Data Act.

[318] *Bundesgesetz über den Schutz personenbezogener Daten* (Federal Act concerning the Protection of Personal Data) (*Datenschutzgesetz* 2000– DSG 2000), which came into force on 1 January 2000.

[319] Article 1(1) of DSG 2000.

[320] Article 1(1) of DSG 2000: 'Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht'.

Also in 2000, Denmark adopted legislation to replace its two Acts dating from 1978, supplanted by a new Act on Processing of Personal Data.[321] In 2001, the Netherlands officially notified the European Commission about the adoption of measures transposing Directive 95/46/EC, in reference to the Dutch Personal Data Protection Act 2000 as amended by supplementary acts of 2001 (European Commission 2003, p. 1). The European Commission thus dropped the proceedings it had launched against Denmark for failure to transpose the Directive in time. Facing the same pressure, France eventually notified the European Commission that its 1978 *loi informatique et libertés* appeared to be somehow consistent with Directive 95/46/EC,[322] while announcing its intention to work on a review (European Commission 2003, p. 1). The Directive was finally incorporated into French law in 2004, with Law Nr. 2004-801 of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data.[323]

Since the 1970s, Germany had already reviewed its Federal Data Protection Act (Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) a number of times. Another revision took place in 2001, and, as Germany notified the European Commission about it, the case opened against it by the Commission was closed.[324] In October 2001, Luxembourg was condemned by the European Court of Justice for failing to transpose within the prescribed period Directive 95/46/EC.[325] The Directive's provisions were finally implemented in Luxembourg through the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data,[326] the purpose of which is defined in terms mirroring those of Directive 95/46/EC (thus, by declaring that the Law aims to protect freedoms and fundamental rights, and notably the right to *vie privée*).[327] A case was brought by the European Commission before the European Court of Justice also against Ireland, in 2001.[328] Ireland

[321] Act No. 429 of 31 May 2000.

[322] Despite the existence of various differences: necessary changes included to fully adapt the notion of *données nominatives* to the notion of personal data (Mallet-Poujol 1999, 54). Arguing the change was not particularly significant: (Ponthoreau 1997, p. 127).

[323] Loi n° 2004-801 du 6 août 2004: Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[324] Ibid. Years later, infringement proceedings on incorrect implementation and application were nevertheless opened against Germany (European Commission, *Commission Staff Working Document Annex to the Communication from the Commission to the Council and the European Parliament "Report on the implementation of The Hague Programme for 2007: Follow-up of the implementation of legal instruments in the fields of Justice, Freedom and Security at national level", 2007 Implementation Scoreboard—Table 2*, SEC (2008) 2048, Brussels, 2.7.2008, 2).

[325] Case C-450/00 *Commission of the European Communities v Grand Duchy of Luxembourg* [2001] ECR I-07069.

[326] *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Mém. A- 91 du 13 août 2002, 1836).*

[327] Article 1 of 2002 Law.

[328] Case C-459/01.

updated its legislation in 2003, with the Data Protection (Amendment) Act,[329] leading to the archiving of the case.

5.3.2 EU Member States Acceding in 2004

The 1990s were also marked in Europe by the activity of former communist countries in Central and Eastern Europe towards the consolidation of their democracies. In this context, many of them adopted provisions on the processing of personal data, and, preparing their accession to the EU in 2004, they soon turned their attention to Convention 108, and to Community legislation.

Hungary addressed data protection issues quickly after the end of its Communist regime. In 1992, it adopted Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest. The main peculiarity of this act is that it serves the double purpose of regulating the protection of personal data, on the one hand, and the implementation of the right of access to data of public interest, on the other.[330] The Hungarian law's framing of personal data protection emphasises the idea of control, by stating that the purpose of the act is to guarantee the right of everyone to exercise control over their personal data.[331] On 26 July 2000, the European Commission decided that Hungarian law ensured an adequate level of protection of personal data within the meaning of Directive 95/46/EC.[332]

Slovenia approved provisions on the protection of personal at the beginning of the 1990s, which were subsequently amended in 1999 with a Personal Data Protection Act.[333] The 1999 Act declares that personal data protection shall prevent any illegal and unwarranted violations of personal privacy in the course of data processing, the securing of personal databases, and the use of data thereof.[334]

In 1996, Estonia enacted a first Personal Data Protection Act (Electronic Privacy Information Center (EPIC) and Privacy International (PI) 2007, p. 421), repealed in 2003 by a new Law on the Protection of Personal Data.[335] The 2003 Law describes its purpose as the protection of the fundamental right and freedoms of natural persons in accordance with public interests,[336] without any reference to privacy

[329] European Commission (2003) op. cit. 1.

[330] Linking this approach to Canadian practice: (Székely 2009, p. 307).

[331] And to have access to data of public interest, except as otherwise provided by law (Article 1(1) of the 1992 Hungarian Act).

[332] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary [2000] OJ L215/4.

[333] *Zakon o varstvu osebnih podatkov, ZVOP, Ur.l. RS No. 59/99.*

[334] Article 1 of the 1999 Slovenian Act.

[335] *Riigi Teataja* (State Gazette) I 1996, 48, 944. For an English translation, see: <http://www.legaltext.ee/text/en/X70030.htm> accessed 20 March 2013.

[336] Chapter 1 § 1 of 1003 Estonian Law on the Protection of Personal Data.

or private life. Lithuania[337] enacted in 1996 a Law on Legal Protection of Personal Data,[338] and ratified Convention 108 in 2001. The purpose of the Lithuanian Law on Legal Protection of Personal Data is to ensure the protection of individuals' right to privacy with regard to the processing of personal data.[339] In 1997, Poland adopted an act on the protection of personal data.[340] In 1998, the Slovak Republic adopted an Act on Personal Data Protection in Filing Systems.[341] The Czech Republic[342] had adopted a similar Act in 1992.[343] It replaced it in 2000 with an Act on Personal Data Protection (Pospíšil and Tichy 2010, p. 4), which formally portrayed itself as being in accordance by EC law.[344] In 2000, Latvia adopted its Personal Data Protection Law, which came into full force in January 2001. In 2001, Romania[345] adopted a Law whose very heading evoked Directive 95/46/EC: Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and free movement of such data.[346] The same year, Cyprus[347] and Malta[348] enacted related legislation.

5.4 Summary

The first steps of EU involvement in the field of data processing regulation were marked by undecided terminology, and unclear perceptions of the role to be played by EU institutions. Encouraged by the European Commission, which emphasised the 'constitutional' dimension of the issue, the European Parliament started to consider the matter with greater detail, leading it to call repeatedly, during the 1970s, for the adoption of Community norms. The European Commission, however, argued then that Convention 108 might be a convenient and sufficient instrument for the purpose of avoiding the potential surfacing of problematic national laws. By the end of the 1980s, nonetheless, and taking into account persisting disparities across

[337] Lithuania signed Convention 108 in 2000, and ratified it in 2001.

[338] Law on Legal Protection of Personal Data, 21 January 2003, No. IX-1296, Vilnius.

[339] According to its Article 1.

[340] Journal of Laws no. 133, item 883.

[341] Act No 52/1998 on Protection of Personal Data in Filing systems.

[342] The Czech Republic ratified Convention 108 in 2001.

[343] Act No 256 on the Protection of Personal Data in Information Systems.

[344] Article 1 of the Czech Act.

[345] Romania ratified Convention 108 in 2001 (Law no. 682/2001 for ratification the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data).

[346] Law No. 677/2001 of 21 of November 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, published in the Official Journal of Romania, Part I No. 790 of the 12th of December 2001.

[347] Law on the Processing of Personal Data (Protection of Individuals) Law 138 (I) 2001.

[348] Maltese Data Protection Act of 2001.

Member States, the European Commission decided to introduce its own legislative proposals on the issue.

The adoption of Directive 95/46/EC in 1995 resulted in the incorporation into EU law of some basic features of existing international instruments. From Convention 108, Directive 95/46/EC took the approach that can be summarised in the formula 'data protection serves (in particular) privacy'. Also from Convention 108, and thus indirectly from the OECD Guidelines, the 1995 Directive imported the idea that, in the area of data processing, it is necessary to balance the protection of individuals with other demands—in this case, the 'free flow' of personal data, envisaged here as a 'fundamental freedom', or a necessary condition for the establishment of the internal market. Other Community norms related to privacy nourished a relative vagueness of the word's meaning.

European integration also progressed through other paths, such as the creation of the Schengen Area and, after the Maastricht Treaty, third pillar cooperation. In this context, instruments involving the processing of personal data regularly referred to Convention 108, and there was also a trend to incorporate instrument-specific provisions, usually under the labels of 'data protection' or 'personal data protection'. Further legal developments, both in primary and secondary law, saw provisions related to the protection of personal data unfurling together with the notion of 'free flow' of personal data, which thus started to move even beyond the concrete context of internal market freedoms through which it had originally entered Community law. On the basis of the wording of Directive 95/46/EC, and seemingly in accordance with the letter of the case law of the ECtHR, the European Court of Justice stressed and strengthened the connection between personal data protection and the right to respect for private life as enshrined by Article 8 of the ECHR.

As Directive 95/46/EC was progressively transposed into Member States, the notions of personal data, and data protection, spread throughout Europe. Only a minority of national legal orders, however, incorporated explicitly the idea according to which 'personal data protection serves (in particular) privacy' as in Directive 95/46/EC, or as in Convention 108. National differences persisted, especially in relation to connections between personal data protection and fundamental rights.

References

Abad Amoros, María Rosa. 2013. El recurso de inconstitucionalidad del Defensor del Pueblo contra la LO 15/99 de Protección de Datos de Carácter Personal. *Alfa Redi Revista de Derecho Informático*. http://www.alfa-redi.org/rdi-articulo.shtml?x=578. Accessed 8 March 2013.

Anarte Borrallo, Enrique. 2003. Sobre los límites de la protección penal de datos personales. *Derecho y Conocimiento* 2:225–254.

Asscher, Lodewijk F., and Sjo Anne Hoogcarspel. 2006. *Regulating Spam: A European perspective after the adoption of the E-Privacy Directive*. The Hague: Asser.

Bancilhon, F., A. Chamoux, A. Grissonnanche, and Louis Joinet. 1979. Le problème personne physique/personne morale. In *Étude sur la confidentialité et la sécurité des données: Rapport final Ã la Commission des Communautés européennes*, ed. Gesellschaft für Mathematik und

Datenverarbeitung (GMD), Institut national de recherche en informatique et en automatique (INRIA), and National Computing Centre (NCC).

Barnard, Catherine, and Simon Deakin. 2000. In search of coherence: Social policy, the single market and fundamental rights. *Industrial Relations Journal* 31 (4): 331–345.

Battista Petti, Giovanni. 2006. *La Costituzione Europea e la tutela civile dei Dirtti Umani (Aggiornato alla Legge 15 Dicembre 2005, N. 280)*. Santarcangelo di Romagna: Maggioli Editore.

Bigo, Didier, Sergio Carrera, Gloria González Fuster, Elspeth Guild, Hert Paul De, Julien Jeandesboz, and Vagelis Papakonstantinou. 2011. Towards a new EU legal framework for data protection and privacy: Challenges, principles and the role of the European Parliament. Policy Department C on Citizens' Rights and Constitutional Affairs of the Directorate General for Internal Policies of the European Parliament.

Boehm, Franziska. 2012. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. Berlin: Springer.

Brouwer, Evelien. 2008. *Digital Borders and Real Rights: Effective Remedies for Third-country Nationals in the Schengen Information System*. Leiden: Martinus Nijhoff Publishers.

Brühann, Ulf. 1999. La Directive européenne relative à la protection des données: Fondements, histoire, points forts. *Revue française d'administration publique* janvier-mars (89): 9–19.

Brun, Alain. 2002. Rapport introductif sur le rôle du droit comparé dans la préparation du dossier concernant la protection des données. In *Le rôle du droit comparé dans l'avènement du Droit européen/The Role of Comparative Law in the Emergence of European Law (Lausanne, 14-15 Avril 2000)*, 107-125. Zurich: Schuthess.

Büllesbach, Alfred, Serge Gijrath, Yves Poullet, and Corien Prins, eds. 2010. *Concise European IT Law (Second edition)*. Alphen aan den Rijn: Kluwer Law International.

Bureau du Parlement Européen. 1974. Procès-verbal de la réunion du 23 avril 1974, Annexe Ad 2, Strasbourg.

Burkert, Herbert. 1979. Organisation et méthodes d'opération des Autorités de Protection des Données. In *Étude sur la confidentialité et la sécurité des données: Rapport final à la Commission des Communautés européennes*, ed. Gesellschaft für Mathematik und Datenverarbeitung (GMD), Institut national de recherche en informatique et en automatique (INRIA), and National Computing Centre (NCC), Section 2.

Busch, Andreas. 2006. From Safe Harbour to the rough sea? Privacy disputes across the Atlantic. *SCRIPT-ed* 3 (4): 304–321.

Bygrave, Lee A. 2002. *Data protection law: Approaching its rationale, logic and limits*. The Hague: Kluwer Law International.

Carlin, Fiona M. 1996. The Data Protection Directive: The introduction of common privacy standards. *European Law Review* 21 (1): 65–70.

Carlos Ruiz, Miguel. 2003. El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo* 7 (14): 7–43.

Cavanillas Múgica, Santiago. 2008. Dos derechos emergentes del consumidor: a no ser molestado y a una interacción informativa. *Revista General de Legislación y Jurisprudencia* 2:175–193.

Chalmers, Damian, Christos Hadjiemmanuil, Giorgio Monti, and Adam Tomkings. 2006. *European Union Law*. Cambridge: Cambridge University Press.

Chalton, Simon. 1997. The transposition into UK Law of EU Directive 95/46/EC (the Data Protection Directive). *International Review of Law, Computers & Technology* 11 (1): 25–32.

Chalton, Simon. 2004. Reflections on Durant v FSA. *Computer Law & Security Report* 20 (3): 175–181.

Church, Peter, and Christopher Millard. 2010. Directive 95/46/EC of the European Parliament and of the Council: The data subject's right to object. In *Concise European IT Law (2nd edition)*, eds. Alfred Büllesbach, Serge Gijrath, Yves Poullet, and Corien Prins, 81-85. Alphen aan den Rijn: Kluwer Law International.

Commission of the European Communities. 1972. The European Community and data processing: Government development aids permitted, information [Competition] 21/72.

Commission of the European Communities. 1973a. Scientific and technological policy programme (submitted to the Council by the Commission on 1 August 1973) COM(73) 1250, Parts I & II, 25 July 1973. *Bulletin of the European Communities* Supplement 14/73.

Commission of the European Communities. 1973b. Communication by the Commission of the European Communities concerning a Community policy for data processing: Information memo P-63/73.

Commission of the European Communities. 1973c. Community policy on data processing (Communication of the Commission to the Council). SEC(73) 4300 final. Brussels.

Commission of the European Communities. 1976. A four-year programme for the development of informatics in the Community (submitted to the Council by the Commission). COM(76) 524 final, Vol. I. Brussels.

Commission of the European Communities. 1982. Communication from the Commission to the Council on Community data-processing policy: Report on the status of Community programmes at 31 May 1982. COM(82) 452 final. Brussels.

Commission of the European Communities. 1990. Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security. COM(90) 314final - SYN 287 and 288. Brussels.

Commission of the European Communities. 1993. White paper on growth, competitiveness, employment: The challenges and ways forward into the 21st century. COM(93) 700. Brussels.

Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data. 1992. Model contract to ensure equivalent protection in the context of transborder data flows with explanatory report (Study made jointly by the Council of Europe, the Commission of the European Communities and International Chamber of Commerce).

Coudray, Ludovic. 2004. Case C-101/01, Bodil Lindqvist. *Common Market Law Review* 41:1361–1376.

Coudray, Ludovic. 2010. *La protection des données personnelles dans l'Union européenne: Naissance et consécration d'un droit fondamental*. Berlin: Éditions universitaires européennes.

Craig, Paul, and Búrca Gráinne De. 2011. *EU Law: Text, Cases and Materials (5th edn.)*. Oxford: Oxford University Press.

Critchell-Ward, Ann, and Kara Landsborough-McDonald. 2007. Data protection law in the European Union and the United Kingdom. *Comparative Law Yearbook of International Business* 29:515–578.

Cuffaro, Vincenzo, and Vincenzo Ricciuto, eds. 1997. *La disciplina del trattamento dei dati personali*. Torino: Giappichelli.

Dammann, Ulrich, and Spiros Simitis. 1997. *EG-Datenschutzrichtlinie: Kommentar*. Baden-Baden: Nomos.

De Brouwer, Frédéric. 1999. Protection des données à caractère personnel: Un nouveau cadre légal belge. *Revue de Droit Des Affaires Internationales* 2:181–206.

De Hert, Paul, and Serge Gutwirth. 2009. Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action. In *Reinventing Data Protection?*, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 3–44. Dordrecht: Springer.

De Schutter, Olivier. 2003. La protection du travailleur vis-à-vis des nouvelles technologies dans l'emploi. *Revue trimestrielle des droits de l'homme* 54:627–664.

Delarue, Jean Marie. 2010. Titre VI Dispositions relatives à la Coopération Policière et Judiciaire en matière pénale. In *Commentaire article par article des Traités UE et CE: de Rome Ã Lisbonne (2ème edition)*, ed. Isabelle Pingel. Bâle: Helbing Lichtenhahn.

Dhont, Jan, María Verónica Pérez Asinari, and Yves Poullet. 2004. *Safe Harbour Decision implementation study*. Namur.

Ehlers, Dirk. 2007. The fundamental freedoms of the European Communities. In *European Fundamental Rights and Freedoms: General Principles*, ed. Dirk Ehlers, 175–225. Berlin: De Gruyter.

Electronic Privacy Information Center (EPIC), and Privacy International (PI). 2007. Privacy & Human Rights 2006: An international survey of privacy laws and developments. Washington, D.C. and London: EPIC/PI.

Elías Baturones, Julio José. 1998. La regulación de los datos sensibles en la Directiva 95/46/EC. *Revista Iberoamericana de Derecho Informático* 23–26:1217–1248.

Epiney, Astrid. 2007. Free movement of goods. In *European Fundamental Rights and Freedoms: General Principles*, ed. Dirk Ehlers, 226–254. Berlin: De Gruyter.

Esquinas Valverde, Patricia. 2010. *Protección de datos personales en la policía europea: El derecho de información sobre los datos y su insuficiente garantía frente a Europol, de acuerdo con la Decisión del Consejo Europeo de 2009, vigente desde Enero 2010*. Valencia: Tirant Lo Blanch.

European Commission. 2003. Analysis and impact study on the implementation of Directive EC 95/46 in Member States: Technical Annex I, accompanying the First Report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 final, Brussels.

Frígols i Brines, Eliseu. 2010. La protección constitucional de los datos de las comunicaciones: Delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho de la intimidad a la luz del uso de las nuevas tecnologías. In *La protección jurídica de la intimidad*, eds. Javier Boix Reig and Ángeles Jareño Leal. Madrid: Iustel.

Frosini, Vittorio. 1982. Bancos de datos y tutela de la persona. *Revista de Estudios Políticos* 30:21–40.

General Secretariat of the Council of the European Communities. 1974. Twenty-second review of the Council's work: 1 January–31 December 1974.

Gentot, Michel. 2000. La protection des données personnelles à la croisée des chemins. In *La protection de la vie privée dans la société de l'information: Tome 3*, ed. Pierre Tabatoni, 24–46. Paris: Presses Universitaires de France.

Gómez Navajas, Justa. 2005. *La protección de los datos personales*. Cizur Menor: Aranzadi.

Guerrero Picó, María del Carmen. 2006. *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Cizur Menor: Thomson Civitas.

Gutiérrez Castillo, Víctor Luís. 2005. Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa. *Derecho y Conocimiento* 3:1–19.

Heil, Helmut. 2010. Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks. In *Concise European IT Law (Second Edition)*, eds. Alfred Büllesbach, Serge Gijrath, Yves Poullet, and Corien Prins, 9–32. Alphen aan den Rijn: Kluwer Law International.

High Level Group on the Information Society (Bangemann Group). 1994. Europe and the global information society: Recommendations to the Corfu European council. *Bulletin of the European Union* Supplement 2/94.

Hijmans, Hielke. 2006. The European Data Protection Supervisor: The institutions of the EC controlled by an independent authority. *Common Market Law Review* 43:1313–1342.

Kingreen, Thorsten. 2011. Fundamental Freedoms. In *Principles of European Constitutional Law* (Revised Second Edition), eds. Armin Von Bogdandy and Jürgen Bast, 515–549. Oxford: Hart Publishing.

Korff, Douwe. 2004. The legal framework: An analysis of the 'Constitutional' European approach to issues of data protection and law enforcement. UK Information Commissioner study project: Privacy & law enforcement.

Kotschy, Waltraut. 2010. Directive 95/46/EC of the European Parliament and of the Council: Exemptions and restrictions. In *Concise European IT Law (2nd edition)*, eds. Alfred Büllesbach, Serge Gijrath, Yves Poullet, and Corien Prins, 76–81. Alphen aan den Rijn: Kluwer Law International.

Kranenborg, Herke. 2008. Access to documents and data protection in the European Union: On the public nature of personal data. *Common Market Law Review* 45 (4): 1079–1114.

Kuner, Christopher. 2009. Developing an adequate legal framework for international data transfers. In *Reinventing data protection*?, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 263–273. Dordrecht: Springer.

Lesmes Serrano, Carlos. 2008. *La Ley de Protección de Datos: Análisis y comentario de su jurisprudencia*. Valladolid: Lex Nova.

Magnusson-Sjoberg, Cécilia. 1999. La mise en oeuvre de la Directive en Suède: Une source de remous juridiques. *Revue française d'administration publique* janvier-mars (89): 37–48.

Mallet-Poujol, Nathalie. 1999. La réforme de la Loi 'Informatique et Libertés'. *Revue française d'administration publique* janvier-mars (89): 49–62.

Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.

Moreham, N. A. 2001. Cases: Douglas and others v Hello! Ltd—The protection of privacy in English private law. *The Modern Law Review Limited* 64 (5): 767–774.

Morijn, John. 2006. Balancing fundamental rights and common market freedoms in Union law: Schmidberger and Omega in the light of the European constitution. *European Law Journal* 12 (1): 15–40.

Murillo, de la Cueva, and Lucas Pablo. 2009. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. In *El derecho a la autodeterminación informativa*, eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 11–80. Madrid: Fundación Coloquio Jurídico Europeo.

Niger, Sergio. 2006. *Le nuove dimensioni della privacy: Dal diritto alla riservatezza alla protezione dei dati personali*. Padova: CEDAM.

O' Cinneide, Colm, Myriam Hunter-Henin, and Jörg Fedke. 2006. 'Privacy' in J. M. Smits (ed), (Edward Elgar 2006). In *Elgar Encyclopedia of Comparative Law*, ed. J. M. Smits, 554–565. Cheltenham: Edward Elgar.

Oliver, Peter. 2009. The protection of privacy in the economic sphere before the European Court of Justice. *Common Market Law Review* 46:1443–1483.

Oreja Aguirre, Marcelino, and Francisco Fonseca Morillo. 1998. *El Tratado de Ámsterdam: Análisis y comentarios, Volumen I*. Madrid: McGraw Hill.

Papapavlou, George. 1992. Latest developments concerning the E.C. draft Data Protection Directives. In *Recent developments in data privacy law*, ed. Jos Dumortier, 29–57. Leuven: Leuven University Press.

Pearce, Graham, and Nicholas Platten. 1998. Achieving personal data protection in the European Union. *Journal of Common Market Studies* 36 (4) (December): 529–547.

Peers, Steve. 2006. *EU Justice and Home Affairs law (2nd Edition)*. Oxford: Oxford University Press.

Pino, Giorgio. 2002. Giudizi di valore e dottrine civilistiche: Il caso dei diritti della personalità. *Diritti & Questioni Pubbliche* 2 (agosto): 132–173.

Pino, Giorgio. 2006. Il Diritto all'identità personale ieri e oggi: Informazione, Mercato, dati personali. In *Libera circolazione e protezione dei dati personali*, ed. Rocco Panetta. Milano: Giuffrè.

Piris, Jean-Claude. 2010. *The Lisbon Treaty: A Legal and Political Analysis*. Cambridge: Cambridge University Press.

Poiares Maduro, Miguel. 1998. *We the Court: The European Court of Justice and the European Economic Constitution: A Critical Reading of Article 30 of the EC Treaty*. Oxford: Hart Publishing.

Ponthoreau, Marie-Claire. 1997. La Directive 95/46 CE du 24 octobre 1995 relative à la Protection des Personnes Physiques à l'égard du Traitement des Données à Caractère Personnel et à la Libre Circulation de ces Données. *Revue Française de Droit Administratif* 13 (1 (janvier–février)): 125–150.

Pospíšil, Filip, and Marek Tichy. 2010. Comparative study on different approaches to new privacy challenges, in particular in the light to technological developments: Country study A.1: Czech Republic. European Commission.

Poullet, Yves, and Serge Gutwirth. 2008. The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: An illustration of 'Reflexive Governance'? In *Défis du droit à la protection de la vie privée: Challenges of Privacy and Data Protection Law*, eds. María Verónica Pérez Asinari and Pablo Palazzi. Bruxelles: Bruylant.

Raab, Charles D., Colin J. Bennett, Robert M. Gellman, and Nigel Walters. 1999. *Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer*. European Commission.

Regan, Priscilla M. 2003. Safe harbors or free frontiers? Privacy and transborder data flows. *Journal of Social Issue* 59 (2): 263–282.

Ricciuto, Vincenzo. 2011. Consentimiento y autodeterminación informativa: La experiencia italiana. In *Protección de datos personales en la sociedad de la información y la vigilancia*, ed. María Rosa Llácer Matacás, 39–59. Las Rozas: La Ley.

Rigaux, François. 1990. *La Protection de la vie privée et des autres biens de la personnalité*. Bruxelles: Bruylant.

Rigaux, François. 2002. What about individual rights in a society of mass information? In *Privacy protection in the information society*, eds. Pierre Tabatoni and François Terré, 35–52. ALL European Academies.

Riolfo Marengo, Silvio, ed. 1993. *Enciclopedia Garzanti del Diritto*. Milano: Garzanti.

Rodotà, Stefano. 2005. *Intervista su Privacy e Libertà a cura di Paolo Conti*. Roma: Editori Laterza.

Saarenpää, Ahti. 2008. Perspectives on Privacy. In *Legal Privacy*, ed. Ahti Saarenpää, 19–63. Zaragoza: Prensas Universitarias.

Seipel, Peter. 1996. Comments on the EC Data Protection Directive: The view from Sweden. *The Journal of Information, Law and Technology (JILT)* 1. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1996_1/seipel/. Accessed 10 March 2013.

Serrano Pérez, Mercedes. 2003. *El derecho fundamental a la protección de datos: Derecho español y comparado*. Madrid: Thomson Civitas.

Simitis, Spiros. 1985. Les garanties générales quant à la qualité des données à caractère personnel faisant l'objet d'un traitement automatisé. In *Informatique et Droit en Europe: Actes du Colloque organisé par la Faculté de Droit avec la participation de l'Association Belge des Juristes d'entreprise les 14, 15 et 16 juin 1984, Bruxelles*, ed. Centre d'informatique appliquée au droit de la Faculté de droit de l'Université Libre de Bruxelles, 305–315. Bruxelles: Bruylant.

Simitis, Spiros. 2006. Einleitung: Geschichte - Ziele - Prinzipien. In *Bundesdatenschutzgesetz*, ed. Spiros Simitis, 61–153. Baden Baden: Nomos.

Solinas, Carla. 2011. Tutela de la persona y tratamiento de los datos personales: Derecho interno y jurisprudencia del Tribunal Europeo de los Derechos Humanos y de las Libertades Fundamentales. In *Protección de Datos Personales en la Sociedad de la Información y la Vigilancia*, edited by María Rosa Llácer Matacás, 133–171. Las Rozas: La Ley.

Spinelli, Altiero. 1974. Letter to Cornelis Berkhouwer, President of the European Parliament, of 21 March 1974, PE 36.587 (BUR), Annexe Ad 9.

Sudre, Frédéric. 2005. *Droit européen et international des droits de l'homme (7th edition)*. Paris: Presses Universitaires de France.

Székely, Iván. 2009. Freedom of information versus privacy: Friends or foes? In *Reinventing Data Protection?*, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 293–316. Dordrecht: Springer.

Szyszczak, Erika, and Adam Cygan. 2008. *Understanding EU Law*. London: Sweet & Maxwell.

Teenage Fanclub. 1990. Everything Flows. *A Catholic Education.* Matador.

Thierry, Léonard, and Yves Poullet. 1999. La protection des données à caractère personnel en pleine (r)évolution: La Loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 Octobre 1995. *Journal des Tribunaux* 118 ((5928, 22 mai 1999)): 377–396.

Thomas-Sertillanges, Jean-Baptiste, and Elisabeth Quillatre. 2011. Libre circulation des données à caractère personnel au sein du marché intérieur et de l'espace de Liberté Sécurité Justice: Vers une diversification des instruments de régulation. *Petites Affiches* 400:3–9.

Wacks, Raymond. 1989. *Personal Information: Privacy and the Law*. Oxford: Oxford University Press.

Walker, Neil. 2004. In search of the Area of Freedom, Security and Justice: A constitutional Odyssey. In *Europe's Area of Freedom, Security and Justice*, ed. Neil Walker. Oxford: Oxford University Press.

Walter, Christian. 2007. The notion of European fundamental rights and freedoms. In *European fundamental rights and freedoms*, ed. Dirk Ehlers, 1–24. Berlin: De Gruyter.

Westin, Alan F. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues* 59 (2): 431–453.

Wong, Rebecca, and Joseph Savirimuthu. 2008. All or nothing: This is the question? The application of art. 3(2) Data Protection Directive 95/46/EC to the internet. *John Marshall Journal of Computer & Information Law* 25 (2): 241–266.

Zerdick, Thomas. 1995. European aspects of data protection: What rights for the citizen? *Legal Issues of European Integration* 2:59–86.

Chapter 6
EU Fundamental Rights and Personal Data Protection

Mother came rushing in.
She said we didn't see a thing.
We said we didn't see a thing.

(Smog 1999)

While developing its involvement in the regulation of data processing, the European Union (EU) was also redefining its approach to fundamental rights. In this field, the EU moved from an initial reluctance to even consider any issues related to fundamental rights, towards an explicit recognition of some of these rights as general principles of law, and, later, towards the formulation of its own rights' catalogue. In this process saw the light a right to the protection of personal data, recognised as 'fundamental'.

This chapter focuses on the inscription of personal data protection among the emergent category of fundamental rights of the EU. It first addresses the question of the nature of EU fundamental rights. Second, it reviews the irregular recognition of personal data protection as a fundamental right in EU Member States, questioning the possible existence of a common constitutional tradition on the subject. Third, the chapter explores the surfacing of personal data protection in tentative listings of EU fundamental rights. Finally, it examines the elaboration of the EU Charter of Fundamental Rights, and describes the integration of the protection of personal data in this text.

The chapter is thus directly concerned with explaining how could the EU consider the possibility to endorse a EU-specific catalogue of rights that it called 'fundamental', and how could personal data protection, as a right not previously recognised in any formally acknowledged source of EU fundamental rights, end up in such a catalogue.

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_6,

6.1 The EU and Fundamental Rights

The original Treaties establishing the European Communities did not contain any explicit reference to human or fundamental rights.[1] During many years, the European Court of Justice (ECJ), based in Luxembourg and maximum interpreter of the law of the European Community (EC), unambiguously portrayed itself as unconcerned with this category of rights. In 1959, for instance, the Court held that it lacked competence to examine whether a European Coal and Steel Community decision constituted an infringement of fundamental rights as recognised by the Constitution of a Member State.[2]

The entanglement of EU law and fundamental rights was progressive, and directly stimulated by a resistance of national legal systems to the impact of EU law, which advanced itself as *supreme*.[3] Reticent Member States eventually accepted the supremacy of EU law only on the condition that EU law would respect their fundamental rights. In its turn, the EU developed a system of fundamental rights protection that promised precisely to do so, even if only indirectly: not by guaranteeing the insurance of national fundamental rights, but rather of EU fundamental rights, nevertheless partially inspired in the common national traditions of the Member States. Thus, EU law eventually created, based on demands emanating from Member States for it to ensure respect for (national) fundamental rights, its own fundamental rights.

6.1.1 Demarcating Fundamental Rights

The expression 'fundamental rights' is commonly used to allude to rights that are granted a special status by a certain legal order (Pérez Luño 2010, p. 569). The legal order in question is often a national legal order, but this does not need to be so (Pérez Luño 2010, p. 569). And their special status is generally a reinforced protection established by a constitutional norm, but this is not always the case (Pérez Luño 2010, p. 33 and 569). Normally, constitutional norms configure fundamental rights as being at least partially out of the legislator's reach, who should not be able to undermine

[1] Apart from provisions on the free movement of workers, and on equal pay between men and women, linked to the needs of economic integration (De Schutter 2010, p. 23). The Treaty of Rome, signed on 25 March 1957 and entered into force on 1 January 1958, included a reference to 'peace and liberty' in Recital 8: 'Member States are resolved to preserve and strengthen peace and liberty'. The possible inclusion of provisions on rights had briefly surfaced in the early 1950s in discussions on the foundations of the upcoming organization, but was eventually put aside. See, on initial considerations: (De Búrca 2011). De Búrca notably refers to the role of Altiero Spinelli, who pointed out to the members of the *Comité d'études pour la constitution européenne* (CECE) the opportunity to give attention to *'les droits de l'homme et des libertés fondamentales*' ('human rights and fundamental freedoms').

[2] C-1/58 *Stork & Cie. v High Authority* [1959] ECR 43, Judgment of the Court of 4 February 1959.

[3] On the supremacy of law, see, for instance: (Craig and De Búrca 2011, pp. 256–300).

them. Additionally, special procedural safeguards might be in place to protect these rights (De Domingo 2011, p. 24).

The alluded linkage between fundamental rights and national legal orders mirrors the fact that especially protected rights recognised in international law will more often be referred differently, namely as 'human rights' (Pérez Luño 2010, p. 33). This difference in terminology can be explained in reference to the very terminology of many international law instruments, which tend to rely on the idiom human rights (and others such as *Menschenrechte, droits de l'homme, diritti umani*).[4] In the Anglo-Saxon world, the distinction is often mirrored by the opposition between human rights and civil rights (Morange 2003, p. 950).

In international legal instruments, occurrences of the expression fundamental rights are relatively rare.[5] The Universal Declaration of Human Rights (UDHR), adopted by the UN General Assembly on 10 December 1948, explicitly mentions fundamental rights,[6] but not to refer to the rights listed in its own provisions, which were labelled as human rights (Dreyer 2006). The expression fundamental rights is used instead in reference to the fact that everyone has the right to an effective remedy by national tribunals for acts violating the 'fundamental rights' granted to them 'by the constitution or by law'.[7]

The usage of the label fundamental rights to describe rights especially protected by national legal orders is also commonly associated with the influence of the German doctrine about *Grundrechte* ('fundamental rights') (Pérez Luño 2010, p. 33). This doctrine envisions the existence of a strong connection between fundamental rights and the State, granting them a funding role of the legal systems of constitutional societies (Pérez Luño 2010, p. 569). The doctrine started to develop in Germany already before the Second World War, and culminated in the adoption in 1949 of the *Grundgesetz für die Bundesrepublik Deutschland* (Fundamental Law for the Federal Republic of Germany),[8] which recognises fundamental rights as directly applicable.[9] The *Grundgesetz* takes away from ordinary legislative procedures the entire area of fundamental rights, adopting a model of rigid Constitution that puts

[4] On the difficulties of translating these notions: (Bellos 2011, pp. 229–233).

[5] The Charter of the United Nations (UN), signed in San Francisco on 26 June 1945, refers for instance in its preamble to 'fundamental human rights' ('We the peoples of the United Nations determined (…) to reaffirm faith in fundamental human rights…'), and later in its provisions to 'human rights' and 'fundamental freedoms' (Article 1(3) and Article 55(c)).

[6] A reference to 'fundamental human rights' is also present in the preamble, echoing the preamble of the UN Charter ('Whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women…').

[7] Article 8 of the UDHR.

[8] Fundamental Law for the Federal Republic of Germany of 1949. For an English translation, see: ("Basic Law for the Federal Republic of Germany, Translated by Christian Tomuschat and David P. Currie, Translation Revised by Christian Tomuschat and Donald P. Kommers in Cooperation with the Language Service of the German Bundestag" 2010).

[9] Article 1(3) of 1949 Fundamental Law. Note that Article 1(2) also refers to inviolable and inalienable *Menschenrechten* ('human rights') as constituting the basis of every community, of peace and of justice in the world.

the matter in the hands of qualified majorities. It also includes an enhanced control of constitutionality, making the protection of fundamental rights a key task of the Federal Constitutional Court.[10] In addition, fundamental rights are recognised as having an 'essential content'[11] that can never be restricted (Rodotà 2009, p. 19).[12]

The expression fundamental rights gained popularity over the last decades.[13] It was incorporated into the Constitutions of Portugal, Spain, the Netherlands, and Finland (Grewe and Ruiz Fabri 1995, p. 142),[14] and has become nowadays a widely shared reference, despite the persistent variety of denominations which are applied to especially protected rights in national legal systems (Grewe and Ruiz Fabri 1995, p. 142). The expression fundamental rights is also well placed in the case law of different European Constitutional courts, including in Common law Member States (Moderne 2000, p. 58). In France, the phrase originally failed to play an important role in modern Constitutional texts, even though its roots (as *droits fondamentaux*) are sometimes located in French pre-revolutionary debates (Dreyer 2006, p. 2).[15]

The 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) does not include any reference to fundamental rights. The European Court of Human Rights (ECtHR), its maximum interpreter, has however progressively adopted the expression. Since 2000, the Court has been using it relatively frequently in the *ratio decidendi* of its judgments (Dreyer 2006, p. 4). The judges also started to use the expression frequently in their dissident or discordant opinions (Dreyer 2006, p. 5). In 2001, the ECtHR designated as a 'fundamental right of the individual' the privilege it attaches to correspondence between prisoners and their lawyers.[16]

In the EU context, the idiom fundamental rights usually refers to the rights protected by EU law, whereas the expression human rights commonly designates rights recognised in international law. EU law is very attached to the idiom 'fundamental freedoms', which has traditionally alluded in EU law to the basic freedoms of the common market: the free movement of goods, persons, services and capital (De Witte 1999, p. 863).[17] EU law has never provided a general definition of fundamental rights. Their current recognition is profoundly indebted to their historical unearthing by the European Court of Justice.

[10] Article 93 of 1949 Fundamental Law. See also: (Schneider 1979, p. 12).

[11] Or *Wesensgehalt*; Article 19(2) of 1949 of Fundamental Law.

[12] This idea of fundamental rights having an essential content was later incorporated into various European constitutional texts (De Domingo and Martínez-Pujalte 2011, p. 31).

[13] Displacing other idioms such as 'inviolable rights' (Rodotà 2009, p. 32).

[14] See also: (Moderne 2000, p. 57).

[15] The expression *droits fondamentaux* is believed to have emerged around 1770 (Dreyer 2006, p. 2).

[16] Erdem v Germany [2001] ECR 2001-VII, App. No 38321/97, § 65. In the original French version of the judgment: *'la correspondance entre un détenu et son défenseur constitue un droit fondamental pour un individu'*.

[17] See also: (Picod 2000, p. 141; Walter 2007, p. 18).

6.1.2 The Discovery of EU Fundamental Rights

The ECJ's initial refusal to rule on the compatibility of Community law with national fundamental rights was perceived as highly problematic by a number of Member States, which, in the name of the supremacy of Community law, had de facto been deprived of the possibility to put into question the validity of Community law themselves. By the end of the 1960s, the ECJ decided to abandon its controversial position. The Court started to assert that fundamental rights were an integral element of the general principles of the law of the European Communities, which it is bound to ensure. Three judgments marked this jurisprudential change: *Stauder*,[18] in 1969; *Internationale Handelsgesellschaft,*[19] in 1970; and *Nold II*,[20] in 1974. In these three landmark judgments, the Luxembourg Court established the doctrine according to which fundamental rights are an integral part of the general principles of EU law, and that, in order to identify such fundamental rights that are to be protected as general principles of EC law, it draws inspiration from the constitutional traditions common to the Member States, as well as from international treaties for the protection of human rights on which Member States have collaborated, or of which they are signatories.[21]

Even though this jurisprudential move had been motivated by the Member States apprehensions on the compatibility of EC law with the fundamental rights protected by their legal systems, the ECJ never pretended to be directly concerned with the insurance of national fundamental rights. The rights that the ECJ was to ensure as general principles of Community law were rights that it identified by its own means, taking into account its own assessment of common national constitutional traditions, and its own reading of the ECHR. Common constitutional traditions and the rights of the ECHR were thus configured as secondary sources of cognition for determining unwritten Community standards,[22] not as direct sources of (EU) fundamental rights.

The *Stauder* judgment is particularly illustrative of this fact. It concerned a request for a preliminary ruling regarding a Decision of the Commission of the European Communities[23] authorising Member States to make butter available at a discounted price to certain categories of consumers. The plaintiff in the main action was a victim of the Second World War who was, as such, a potential beneficiary of the discounted butter. In application of the German version of the Commission

[18] C-29/69 *Stauder v Stadt Ulm* [1969] ECR 419, Judgment of the Court of 12 November 1969.

[19] C-11/70 Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel [1970] ECR 1125, Judgment of the Court of 17 December 1970.

[20] C-4/73 *Nold KG v Commission* [1974] ECR 492, Judgment of the Court of 14 May 1974 (hereafter, '*Nold II*').

[21] *Nold II* § 4.

[22] *Rechtserkenntnisquelle* in German legal doctrine (Walter 2007, p. 12).

[23] Decision No 69/71 EEC of the Commission of the European Communities, adopted in Dutch, French, German and Italian, the four official languages of the EC at that time (Horspool 2006, p. 166).

Decision, the plaintiff was allowed to buy butter at the discounted price in Germany only on the condition of identifying himself to the sellers by disclosing his full name and personal address. Being of the opinion that such obligation constituted an infringement of the fundamental rights enshrined in the German Basic Law, he had introduced a constitutional complaint to the German Federal Constitutional Court.[24] In the request for a preliminary ruling that the ECJ had to deal with, however, the Court was not asked to judge on such possible infringement of the German Basic Law. Instead, the ECJ had to answer a question referred by another court also addressed by the plaintiff, the *Verwaltungsgericht Stuttgart* (Stuttgart Administrative Court), which had opted to ask the ECJ whether the decision of the Commission of the European Communities making the sale of butter at a reduced price dependent on revealing the beneficiary's name to the sellers could be considered compatible with the general principles of Community law in force.

To answer this question, the ECJ first noted that there were differences in meaning between the various official linguistic versions of the Commission Decision at stake, even though these linguistic versions were all authentic and legally binding. Observing that only the German version obliged beneficiaries to actually disclose their names, the Cour advanced that this version could not be read in isolation, but that it should be interpreted taking into account the legislator's intention, which was actually not to oblige beneficiaries to disclose their identities. For the ECJ, the Commission Decision at stake, read in such fashion, contained nothing capable of prejudicing the 'fundamental human rights'[25] enshrined in the general principles of EC law. Thus, the ECJ proved that, although it was not examining the validity of EC law in the light of the rights of any particular Member State, it was ready to assess EC law's validity from the perspective of Community general principles, which happened to include the insurance of (some, at least) national fundamental rights.

In reality, during many years the ECJ appeared to try to hold to a precarious balance between, on the one hand, a tendency to affirm the autonomy of EC fundamental rights, and, on the other hand, a propensity to stress the belonging of such fundamental rights to the national constitutions of Member States (Cartabia 2007, p. 29). In its 1974 judgment for *Nold II*, the Luxembourg Court stated that the fact that it draw inspiration from constitutional traditions common to the Member States in order to safeguard fundamental rights meant that it could never uphold measures 'which are incompatible with fundamental rights recognized and protected by the Constitutions of those States'.[26]

The German Federal Constitutional Court, however, made it clear in 1974 that from its point of view the described jurisprudential turn of the ECJ did not render the situation completely satisfactory. The Federal Constitutional Court proclaimed

[24] Opinion of Advocate General Roemer in C-29/69 *Stauder* [1969] ECR 419.

[25] The English translation of the judgment uses the expression 'fundamental human rights', as an attempt to mirror the German original '*Grundrechte der Person*' (translated in Dutch as '*de fundamentele rechten van de mens*'; in French, '*les droits fondamentaux de la personne*', or, in Italian, '*i diritti fondamentali della persona*').

[26] *Nold II* § 4.

that it would continue to consider the German Fundamental Law superior to EC law until the latter included a written catalogue of fundamental rights.[27] EC institutions seemed to have two possible solutions to overcome the situation: either to commit formally to any existing written catalogue of rights, such as the ECHR, or to produce their own catalogue.

Already in 1975, the possible creation of a new list of rights was advanced in a discussion paper on the future of the European Communities, titled *Report on the European Union*, prepared by the Belgian Leo Tindemans.[28] The report suggested that a list of rights should be incorporated into the basic acts on which the future Union was to rest (Commission of the European Communities 1975, p. 26). In 1976, the European Commission launched a study to examine the problems posed by the elaboration of a catalogue of fundamental rights for the EC (Bernhardt 1976, p. 18), and made public a special report (Commission of the European Communities 1976).

In 1977, the European Parliament, the Council and the European Commission signed a Joint Declaration[29] formally endorsing the new ECJ position, by declaring themselves bound by fundamental rights as general principles of Community law. They stressed 'the prime importance they attach to the protection of fundamental rights, as derived in particular from the constitutions of the Member States and the European Convention for the Protection of Human Rights and Fundamental Freedoms'.[30]

The ECJ case law was later further refined. This refinement culminated at the beginning of the 1990s in the *ERT* judgment (Morijn 2006, p. 18), which confirmed that fundamental rights form an integral part of the general principles of law, the observance of which the Court ensures, and added that '(f)or that purpose the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories (…). The European Convention on Human Rights has *special significance*[31] in that respect'.[32]

As general principles of EU law, fundamental rights are primarily binding on the EU (Ehlers 2007a, p. 182). But they also bound Member States when these apply EU law. The doctrine known as 'incorporation' refers to the case law of the ECJ which, since the end of the 1980s, started to broaden the scope of application of EU fundamental rights, and thus also the number of cases in which the Court regarded

[27] The German Federal Constitutional Court also found critical the lack of a viable legislative power (the 'democratic deficit' of the EC); see: BVerfGE 37, 271 2 BvL 52/71 *Solange I*-Beschluß.

[28] Generally known as the Tindemans Report. See: (Commission of the European Communities 1975). Leo Tindemans had been instructed by the Paris Summit of 9 and 10 December 1974 to draw up a report on the interpretation of the term 'European Union'.

[29] Joint Declaration by the European Parliament, Council and the Commission concerning the protection of fundamental rights and the ECHR, Luxembourg, 5 April [1977] OJ C103/1.

[30] Ibid.

[31] Emphasis added.

[32] C-260/89 *ERT v DEP* [1991] ECR I-2925, Judgment of the Court of 18 June 1991, § 41.

itself competent to adjudicate on the compliance of national measures with the fundamental rights it protects. As a result, two key types of national measures are to be regarded as falling under the scope of application of EU law: those adopted when Member States apply directly EU law (the so-called *Wachauf* line[33]), and those adopted by Member States with the effect of limiting one of the fundamental economic freedoms of the EU (the so-called *ERT* line) (Cartabia 2007, p. 27). Therefore, Member States must respect the fundamental rights which are part of EU law also when they adopt measures derogating from EU law (Craig and De Búrca 2011, p. 384).

6.1.3 Identifying EU Fundamental Rights

The two key secondary sources from which the Luxembourg Court draws inspiration to identify fundamental rights to be ensured as general principles of EU law are thus the common constitutional traditions of the Member States, and international human rights treaties, among which the ECHR is regarded as having special significance.[34]

6.1.3.1 The ECHR

The ECHR, despite not being binding on the EU as such, eventually became the main material source used by the ECJ for the identification of fundamental rights (Sudre 2005, p. 143). More concretely, the ECJ references often ECtHR's case law on the ECHR, case law that it routenily expressly quotes (Sudre 2005, p. 145). Although the Luxembourg Court generally does so in what has been portrayed as a deferential approach (Harpaz 2009, p. 110), aimed at avoiding any possible conflict of interpretation (Pernice and Kanitz 2004, p. 13), the Court interprets the ECHR and ECtHR case law in an autonomous way, in the specific context of EU law (Sudre 2005, p. 144). Differences in interpretation between the ECtHR and the ECJ can emerge. In practice, some of them are indeed believed to have appeared (Wetzel 2003, p. 2843), in particular in relation with the interpretation of Article 8 of the ECHR, a provision invoked since the beginning in a relatively high number of actions brought before the Luxembourg Court (Guild and Lesieur 1998, p. xxii).

In *National Panasonic,*[35] the Luxembourg Court had to deal with a contentious claim according to which there had been an infringement of Article 8 of the ECHR.

[33] In reference to C-5/88 *Wachauf v Bundesamt für Ernährung und Forstwirtschaft* [1989] ECR 2609 Judgment of the Court (Third Chamber) of 13 July 1989.

[34] The ECJ first used the ECHR to obtain indications (C-36/75 *Rutili v Ministre de l'intérieur* [1975] ECR 1219, Judgment of the Court of 28 October 1975, § 32) and later granted to the ECHR a particular significance (C-46/87 *Hoechst v Commission* [1989] ECR 2919, Judgment of the Court of 21 September 1989, § 16).

[35] C-136/79 *National Panasonic v Commission* [1980] ECR 2035, Judgment of the Court of 26 June 1980.

The case concerned an application introduced by a company for the annulment of a Commission Decision regarding an investigation made by two Commission officials who had arrived without prior notice at a company's sales offices. The applicant, which was a company, claimed that by failing to communicate beforehand the decision ordering the investigation, the Commission had infringed its fundamental rights. The applicant relied in particular on Article 8 of the ECHR, expressing that it considered that the guarantees granted by this provision should be applied *mutatis mutandis* to legal persons.[36] According to the European Commission, however, the assumption that the principles laid down in Article 8 of the ECHR applied to legal persons was not entirely free from doubt. In its judgment, the Luxembourg Court found a way to ground its legal reasoning on Article 8 of the ECHR (allowing the Court to the declare that, in case there had been an interference, the interference had a legitimate aim),[37] but without explicitly asserting that the provision in question was applicable to legal persons.

In his Opinion for *National Panasonic*,[38] Advocate General Warner had recalled an earlier case, *Brescia,*[39] in which, according to him, the ECJ had 'clearly considered that the right to privacy extends to business premises, whether those of an individual or of a company'.[40] In reality, in that judgment the Luxembourg Court had merely referred, in passing, to the fact the existence of Treaty provisions[41] on the need to regulate some 'inspections, capable of affecting the area of individual liberty and of departing from the principle of the inviolability of private premises',[42] without making any further comments (Lawson 1994, p. 237).

In 1989, in *Hoechst*,[43] the ECJ had to address another claim by a company referring to Article 8 of the ECHR. The applicant sought the annulment of a Decision[44] to carry out an inspection on its premises for suspected participation in a cartel. Relying inter alia on its right to the inviolability of the home under Article 8 ECHR, the applicant submitted that for a search to be lawful, it was necessary for the Commission to have a court order, issued by the ECJ (Lawson 1994, p. 239). In his Opinion on the case,[45] Advocate General Mischo, having reviewed Member State practice in relation to the protection of the home, and the extent to which the

[36] *National Panasonic* § 17.

[37] Noting that whether the investigation had actually been 'necessary in a democratic society' was left unanswered: (Lawson 1994, p. 238).

[38] Opinion of Advocate General Warner in C-136/79 *National Panasonic.*

[39] C-31/59 *Acciaeria e tubificio di Brescia v High Authority* [1960] ECR 153, Judgment of the Court of 4 April 1960.

[40] Opinion of Advocate General Warner in C-136/79, 2068.

[41] In particular, Article 86 of the Treaty establishing the European Coal and Steel Community (Paris, 18 April 1951).

[42] *Brescia* § 3.

[43] C-46/87 *Hoechst v Commission* [1989] ECR 2919, Judgment of the Court of 21 September 1989.

[44] Taken pursuant to Article 14 of Regulation No 17: First Regulation implementing Articles 85 and 86 of the Treaty [1962] OJ 13, 204.

[45] Opinion of Advocate General Mischo in Joined Cases C-46/87 and C-227/88 *Hoechst*.

right included business premises,[46] observed a general trend in national legal systems towards the assimilation of business premises to the notion of home. Advocate General Mischo consequently invited the Court to expressly accept the existence at Community level of a fundamental right to the inviolability of business premises (Lawson 1994, p. 240).

The Luxembourg Court, however, rejected the applicant's contention, on the grounds that the 'home' in this context referred exclusively to the 'private dwellings of natural persons'. The Court explicitly stated that there existed a fundamental right to the inviolability of the home recognised in the Community legal order as a principle common to the laws of the Member States, but only 'in regard to the private dwellings of natural persons', as opposed to 'undertakings'.[47] The ECJ also explicitly asserted that no other inference was to be drawn from Article 8 of the ECHR.[48] Nonetheless, the Court accepted as a general principle of Community law that 'intervention by the public authorities in the sphere of private activities of any person, whether natural or legal, must have a legal basis and be justified on the grounds laid down by law'.[49]

After *Hoechst*, the ECJ was criticised for having overlooked a case decided by the ECtHR a few months earlier, *Chappell*,[50] which allegedly extended the protection of Article 8 of the ECHR to undertakings (Lawson 1994, p. 241). In reality, the *Chappell* ruling was ambiguous in that respect: the case concerned a search directed against the applicant's company, but focused mainly on the interference with the applicant's home envisaged jointly with his private life (Lawson 1994, p. 241). The Strasbourg Court had asserted that the scope of application of Article 8 of the ECHR could encompass some protection in relation with the professional premises of individuals, but had not decided on the applicability of the inviolability of the home in relation with legal persons (Briboisia and Van Drooghenbroeck 2009, p. 162).

The ECtHR addressed the issue of protection related to professional premises in 1992, in *Niemietz* (Rincón Eizaga 2008, p. 137), a case where the applicant was an individual complaining about searches carried out at his office. Here, the Strasbourg Court declared that the scope of Article 8 of the ECHR covers certain professional or business activities or premises, and held that the measure at stake was an interference that could not be regarded as 'necessary in a democratic society' (Lawson 1994, p. 243). In *Roquette Frères*, the Luxembourg Court acknowledged that, in the light of *Niemietz* (Mischo 2003, p. 139), its ruling in *Hoechst* could no longer stand, and accordingly modified its position (Douglas-Scott 2006, p. 649). The ECJ, nonetheless, cited a passage in *Niemietz* in which the ECtHR had asserted that the discretion enjoyed by the Contracting Parties under Article 8(2) of the ECHR was

[46] Ibid.

[47] *Hoechst* § 17.

[48] Ibid. § 18.

[49] Ibid. § 19.

[50] *Chappell v the United Kingdom* [2002] Series A No 152-A, App No 10461/83. See: (Rincón Eizaga 2008, p. 137).

particularly significant in relation to professional or business activities (Oliver 2009, p. 1481).[51]

Another question that has generated apparent mismatches between the Luxembourg and the Strasbourg Court concerns the right of individuals to respect for their name.[52] Although described as showing that case laws of the ECJ and the ECtHR can be 'at odds' (Douglas-Scott 2006, p. 643), or even in 'flagrant conflict' (Spielmann 1999, p. 766), these situations have typically surfaced only when the Luxembourg Court rules on an issue upon which there is no established Strasbourg case law yet (Lawson 1994, p. 246; Douglas-Scott 2006, p. 649). In this sense, rulings such as *Hoechst* can also be regarded as examples not of divergence, but rather of the Luxembourg's Court will to systematically take into account the ECHR and the relevant ECtHR case law, even in the special situations when such case law does not exist as such (Briboisia and Van Drooghenbroeck 2009, p. 162). Ultimately, if the Luxembourg Court sometimes diverges in its interpretation from (upcoming) ECtHR case law, it is partly because of its insistence on referring to the ECtHR case law whenever issues related to the ECHR and fundamental rights arise, and even when Strasbourg's case law does not provide (yet) a clear answer to the problem at stake.

In relation to the protection of personal data, Strasbourg's case law can be summarised as establishing that Article 8 of the ECHR provides some protection against the processing of information about individuals, even though the extent of such protection might not be fully coincidental with the scope of application of Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108').[53] From a slightly different perspective, the Luxembourg Court has maintained that on the basis of Article 8 of the ECHR, and of Convention 108, it can be asserted that the general principles of Directive 95/46/EC constituted general principles of EC law even before the Directive's adoption in 1995.[54]

6.1.3.2 Common National Constitutional Traditions

The second source of inspiration used by the Luxembourg Court for the identification of fundamental rights to be protected as general principles of EU law is the

[51] In this series of cases, see also: *Société Colas Est and others v France* [2002] ECHR 2002-III, App. No 37971/97 (Mischo 2003, p. 141). On the question of the applicability of Article 8 of the ECHR to legal persons, see: (Briboisia and Van Drooghenbroeck 2009, p. 163).

[52] Cf. C-168/91 *Konstantinidis v Stadt Altensteig and Landratsamt Calw* [1993] ECR I-01191, Judgment of the Court (Sixth Chamber) of 30 March 1993 (concerning a Greek man complaining about the way in which German authorities had transliterated his name, where the question was addressed in economic terms) and *Burghartz v Switzerland* [1994] Series A No 280-B, App No 16213/90 (on the right to a name as necessary to forming one's identity). See: (Wetzel 2003, p. 2844).

[53] See Chap. 4, Sect. 4.3, of this book.

[54] C-369/98 *Fisher* [2000] ECR I-6751, Judgment of the Court (Fourth Chamber) of 14 September 2000, § 34.

notion of common national constitutional traditions. This notion bounds the Court to the ensuring the fundamental rights that it identifies as part of a set of rights regarded as essential across Member States. Because of its lack of clear correspondence with any particular pre-established set of rights, the notion of common constitutional traditions has been qualified as ambiguous and problematic, and accused of opening more questions than it solves (Blanchard 2001, p. 166). The Luxembourg Court, nonetheless, has used it regularly, presumably because of the usefulness of its flexibility.[55] The notion appears as especially relevant in those cases where the ECHR does not explicitly enshrine a particular right, or a particular facet of a right (Ehlers 2007b, p. 374).

In practice, to determine whether a right can be considered as integral to the common constitutional traditions of Member States, the Luxembourg Court makes a (rapid) comparative analysis (Blanchard 2001, p. 166).[56] In relation to the protection of personal data, the Luxembourg Court has never declared that common national constitutional traditions might include ensuring a fundamental right to personal data protection.

6.2 Data Protection and National Constitutional Traditions

Nowadays, all EU Member States have laws on the protection of personal data. And these laws are generally always somehow connected to rights regarded as being of constitutional or equivalent importance (Korff 2010, p. 5). There are, however, substantial differences in how Member States conceive of this framing. In some cases, the fundamental rights dimension of personal data provisions is strictly derived from their linkages with rights in the international and European instruments to which they are associated, such as Convention 108, or Directive 95/46/EC. In others, the fundamental rights dimension signals a connection with rights especially protected by national instruments. And in others still, it takes the shape of an association with a specific, sui generis right, sometimes, but not always, named the right to the protection of personal data.

Based on their approach to the relation between the protection of personal data and fundamental rights, Member States can be classified[57] into the following groups:

[55] For instance, in Joined Cases C-387/02, C-391/02 and C-403/02 *Berlusconi and Others* ([2005] I-3565 Judgment of the Court (Grand Chamber) of 3 May 2005), where the Luxembourg Court found that '[t]he principle of the retroactive application of the more lenient penalty forms part of the constitutional traditions common to the Member States' (§ 68).

[56] Also: (Cremer 2011, p. 9).

[57] For a complementary classification: (Arenas Ramiro 2006, p. 379). As a supplementary comparative analysis of constitutional protection in some Member States, see: (Koops et al. 2007).

A. Member States where the protection of personal data is conceived as primarily serving other existing rights (for instance, Belgium, where it is regarded as pursuing the insurance of 'privacy');
B. Member States where the protection of personal data is connected to a *sui generis* fundamental right, recognised explicitly in the Constitution, or in a norm with constitutional status (for instance, Hungary, Slovakia, or the Czech Republic);[58]
C. Member States where there exists in the Constitution a specific mandate to legislate on the protection of personal data (such as in the Netherlands, or in Finland);[59]
D. Member States where the Constitution does not overtly address the protection of personal data, but where the Constitutional Court has established the existence of a sui generis right with a relatively similar content (for instance, in Germany);
E. Member States where the linkage between personal data protection and fundamental rights is uncertain (as in Denmark).

This taxonomy is primarily indicative. In reality, in the majority of cases it is difficult to ascribe national approaches to a specific model. Even when a Member State formally recognises the existence of a sui generis right (as in group B), it might nevertheless envision this right as not autonomous but rather as serving another right, with an effect equivalent to framing personal data protection laws as implementing another right (as in the A group). A paradigmatic example of this situation is Austria.

6.2.1 Separate Protection

A significant number of EU Member States that nowadays recognise explicitly a right to the protection of personal data entered the EU only in 2004– thus, after the right's inscription as EU fundamental right in the EU Charter of Fundamental Rights of 2000. When the EU Charter was being drafted, only a few Member States had adopted this approach.

Portugal incorporated provisions on the automated processing of personal data already in its Constitution of 1976, in Article 35. Article 35 is often referred to as establishing a right to the protection of personal data,[60] but it does not explicitly endorse this nomenclature: its heading alludes to the 'use of computers' (*utilização da informática*). Article 35 of the Portuguese Constitution originally comprised three paragraphs, but was later reviewed and expanded (Dias Venâncio 2007, p. 244). In 1982, a Constitutional review added a paragraph stating that computers shall not be used to process data about philosophical or political opinions, membership of political party or trade union, religious faith or private life (*vida privada*), except when processed for statistical purposes in a non-identifiable form;[61] as well as another

[58] Portugal could be included in this group, even if it Constitution does not explicitly refer to a right to the protection of personal data.

[59] Spain could be regarded as pertaining to this group, except that the Spanish Constitutional Court has interpreted the legislative mandate of the Spanish Constitution in the sense that it enshrines a fundamental right to the protection of personal data.

[60] See, for instance: (Silveira 2007).

[61] Article 27(3) of Lei Constitucional 1/1982, de 30 de Setembro.

paragraph stating that data transfers to third countries could only occur exceptionally.[62] In 1989, coinciding with a second Constitutional revision,[63] a number of changes were incorporated, notably to the effect of merely stating that law shall define the regime applicable to transborder data flows, no longer viewed as exceptional.[64] Article 35 acquired its current form with the Constitutional review of 1997.[65] Since then, the paragraph on special categories of data refers also to ethnic data, but, instead of a general prohibition of processing the types of data explicitly mentioned, it establishes that their processing is possible if on the basis of the explicit consent of individuals, or on the basis of a law foreseeing appropriate safeguards against discrimination.[66] The 1997 review took into account the adoption of Directive 95/46/EC, which granted protection not only to data being automatically processed. Now, a last paragraph establishes that manual files shall enjoy exactly the same level of protection as described in the other paragraphs of Article 35.[67]

Since 1983, Germany recognises a right related to the processing of personal data, which is nevertheless not designated as a right to the personal data protection (despite the German roots of the expression 'data protection'), but as a *Recht auf informationelle Selbstbestimmung*,[68] or 'right of informational self-determination'. The right was identified by the German Federal Constitutional Court[69] in the landmark *Volkszählungsurteil*,[70] a judgment surfaced in the context of reactions to plans by the German government to carry out a census implying the collection of detailed information about individuals.

The German Federal Constitutional Court had already dealt with the processing of personal data in 1969, in its *Mikrozensus* judgment.[71] Already then, the Court had considered the protection of individuals against the processing of data as falling under the right to dignity, as established by Article 1(1) of the Fundamental Law, read in conjunction with its Article 2(1), on the free development of personality. The Court has traditionally based on these two provisions the recognition of a general right to freedom of action (Alexy 2010, p. 223),[72] referred by the Court as pertaining to a general right of personality (Hornung and Schnabel 2009, p. 86). Whereas in 1969 the Federal Constitutional Court had addressed the processing of personal

[62] Ibid. Article 27(2).

[63] *Lei Constitucional 1/1989 [DR I série Nº.155/V/2 Supl.1989.07.08]*.

[64] Article 20(4) of *Lei Constitucional 1/1989*.

[65] Lei Constitucional 1/1997 [*DR I série A Nº.218 1997.09.20*].

[66] Or for statistical purposes as mentioned above: Article 35(3) of Portuguese Constitution.

[67] Article 35(7) of Portuguese Constitution.

[68] The invention of the expression has been traced back to 1976 (Burkert 1999, p. 49).

[69] *Bundesverfassunsgericht* (BVerfG).

[70] *Urteil des BVerfG v. 15.12.1983 zum VZG 83* (1 BVerfGE 65).

[71] *Mikrozensus-Urteil,* 16.07.1969 (1 BVerfGE 27, Rn. 20).

[72] See in particular the 1957 Elfes judgment (6 BVerfGE 32), where the German Federal Constitutional Court declared that the free development of personality must be broadly understood, and goes beyond the mere development within a central area of personality (Kommers 1997).

data from the perspective of the 'theory of the spheres',[73] in 1983 it abandoned this theory, opting instead to assert the existence of a *Recht auf informationelle Selbstbestimmung* portrayed as a manifestation of the general right derived from the joint reading of Article 1(1) and Article 2(1) of the Fundamental Law (Hornung and Schnabel 2009, p. 86).[74] Considering that individuals can be limited in their personal development and be affected in their dignity whenever not acting with total freedom, and arguing that individuals would not act with total freedom if they did not know which data about them were being processed, the Constitutional Court introduced such a *Recht auf informationelle Selbstbestimmung* as the possibility for individuals to determine which data about them are processed—a sort of individual decisional authority or power (Kommers 1997, p. 324). The notion of self-determination is in itself a dimension of the free development of personality according to which subjects need to have the capacity to decide autonomously and take free decisions (Arenas Ramiro 2006, p. 382). The right to informational self-determination, argued the Court, is necessary not only from an individual perspective, but also from the perspective of the individual's participation in society (Arenas Ramiro 2006, p. 398). In its judgment, the Federal Constitutional Court defined the core elements of the new right, emphasising that the use of personal must respect a strict limitation of purpose, and that uses incompatible with the purpose of the original collection are to be forbidden (Arenas Ramiro 2006, pp. 401–402). The Constitutional Court explained that limitations to the right were possible, but only if established in law, and if justified in the light of the pursuit of general interests (Arenas Ramiro 2006, p. 399). The Court stressed that the right does not imply that individuals possess an absolute, unlimited mastery over their data (Kommers 1997, p. 325), which, contrario sensu, can be understood as the identification of the right with a relative control or mastery upon personal information.

Years before, in 1978, the German State of North Rhine-Westphalia had introduced in its own Constitutional text a provision on the protection of personal data.[75] The Federal Constitutional Court deviated in 1983 from the widespread use of the idiom data protection to embrace instead 'informational self-determination'. Nevertheless, it repeatedly used in its 1983 judgment expressions such as *persönliche Daten*, *Personaldaten*, or *persönliche Lebensachverhalte* (or existential facts related to the person) (Rigaux 1990, p. 582). The Court expressly drew a distinction between the processing of 'personal data', or data allowing for the identification of

[73] Hinted already in the 1957 *Elfes* judgment. In addition to this theory, and with the same objective, the German doctrine developed also the 'theory of the roles' (*die Rollentheorie),* the 'theory of the autonomous self-representation' (*Die Theorie des autonomen Selbstdarstellung)*, and the 'theory of communication' (*Die Kommunikationstheorie)* (Arenas Ramiro 2006, p. 392).

[74] They are also sometimes referred as specific liberties implied in the Fundamental Law (Rivers 2010, p. xli).

[75] Section 4, paragraph 2, of the Constitution of the Land of North Rhine-Westphalia states that everyone has the right to protection of their personal data, and that infringements are permissible only on the basis of law where the public interest is paramount. Since then, various Länder have followed this path. The Constitution of Berlin, for instance, enshrines the right of individuals to decide on the disclosure and use of personal data (Article 33 of Berlin Constitution).

the person to whom they relate, and processing of anonymous data, which do not allow for such identification (Kommers 1997, p. 326). It noted, however, that both categories of data may have an impact on the individual, as data can be of use for those who process even if they merely refer to facts concerning somebody's life (Kommers 1997, p. 589).

In the Netherlands there is, since the revision of the Dutch Constitution of 1983, a constitutional mandate to legislate on the protection of the general *recht op eerbiediging van zijn persoonlijke levenssfeer* ('right to respect of the personal sphere of life') in relation to the recording and dissemination of personal data, and on the rights to access to and rectification of such data.[76]

In Finland there exists also a mandate to legislate on the protection of personal data, since the mid-1990s.[77] It was included in the Finnish Constitution of 1999[78] with the words: 'More detailed provisions on the protection of personal data shall be laid down by law'.[79] The mandate appears just after a provision establishing that everyone's private life, honour and the sanctity of home are guaranteed, both falling under a Section titled 'the right to privacy'.[80]

In Spain there is since 1978 a Constitutional mandate to legislate on computers, enshrined in Article 18(4) of the Spanish Constitution, which was eventually read by the Spanish Constitutional Court as establishing a fundamental right[81] to the protection of personal data. Already in 1993, the Spanish Constitutional Court had addressed the specificity of Article 18(4) of the Constitution, in a ruling[82] concerning a citizen who had been refused access to data held by the public administration.[83] Although issued after the adoption of a law that placed the protection of personal data under the light of the protection of *privacidad*,[84] the judgment nevertheless avoids the use of this term (Murillo de la Cueva 1999, p. 42). The Constitutional

[76] Article 10 of Dutch Constitution.

[77] Finland undertook a major constitutional review in the mid-1990s, after accession to the ECHR, which led to the increase and broadening of recognised fundamental rights (Prakke and Kortmann 2004, p. 220). The provisions on fundamental rights contained in Chapter II of the new Constitution were reformed in 1995, and later transferred to the new Constitution.

[78] *Perustuslaki* 731/1999 of 11 June 1999.

[79] Unofficial translation of the Constitution of Finland of 11 June 1999 (731/1999, amendments up to 1112/2011 included) published by the Finnish Ministry of Justice <www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf> accessed 8 March 2013. *Referring to it as establishing* '*data protection*': (Saarenpää 1997, p. 49).

[80] Section 10 of Finnish Constitution.

[81] In Spain, the status of fundamental right grants to rights a reinforced protection. Their exercise can only be regulated by law, which must, in any case, respect their essential content (Article 53(1) of the Spanish Constitution). They are also protected through the right of *amparo*, a constitutional guarantee in the form of judicial remedy.

[82] Sentencia del Tribunal Constitucional (STC) 254/1993, de 20 de julio de 1993 (recurso de amparo núm. 1827/1990).

[83] See notably: (Gómez Navajas 2005, p. 110; Guerrero Picó 2006, pp. 208–209; Piñar Mañas 2009, p. 95).

[84] The STC 254/1993 was published a few months after the entry into force of the LORTAD, which was mentioned by the Court. See also: (Orti Vallejo 1994, p. 306).

Court mentioned however *privacy*, using the English word as if it was a noun commonly accepted in Spanish, and advanced such *privacy* as a modern version of the right to *intimidad*. *Privacy*, the Court argued, allegedly constitutes a positive freedom to exercise control on personal data that have left the sphere of *intimidad,* and have become elements of an electronic archive.[85] From there, the Court went on to assert that Article 18(4) of the Constitution enshrined a *libertad informática* ('computer freedom'), which it equated to *habeas data*.[86] In 1998, Spanish Constitutional Court[87] finally asserted the presence of a specific fundamental right in Article 18(4) of the Constitution (Martínez Martínez 2004, p. 302), and advanced it as an autonomous fundamental right[88] concerned with the protection of computerised data.[89]

In Spain, the finding of personal data protection as a fundamental right was consolidated in 2000 (Martínez Martínez 2004, p. 312), in a judgment[90] that overtly took into account relevant international treaties[91] such as the 1990 UN Guidelines for the Regulation of Computerized Personal Data Files[92] and Convention 108, but also Directive 95/46/EC and Article 8 of the EU Charter of Fundamental Rights, which was officially proclaimed only a week later (Sáenz de Santamaría 2008, p. 240). In this ruling, the Constitutional Court put forward the right's core elements,[93] described its boundaries (Martínez Martínez 2004, p. 336),[94] and explicitly referred to it as the *derecho fundamental a la protección de datos*[95] ('fundamental right to

[85] STC 254/1993 § 5.

[86] Ibid. It was the first time that the Constitutional Court used these expressions (Pérez Luño 2010, p. 387). After this conceptual digression, the Constitutional Court nonetheless proceeded with its reasoning by focusing on a possible infringement of the right to *intimidad*, now arguably understood as enriched by the prior considerations on its modernisation—as if hesitating between the assertion of a new right, and a broadening of the right to *intimidad* (Martínez Martínez 2004, 295)—, and ended up providing a very ambiguous judgment (Murillo de la Cueva 2009, p. 32).

[87] STC 11/1998, de 13 de enero de 1998.

[88] STC 11/1998 § 5 (Murillo de la Cueva 1999, p. 46). More precisely, it described Article 18(4) of the Spanish Constitution as establishing a right with a dual nature, both instrumental and autonomous (Solanes Corella and Cardona 2005, p. 27). Considering that this duality is not alien to fundamental rights, an that it increases their significance: (Murillo de la Cueva 1999, p. 47).

[89] STC 11/1998 § 5.

[90] STC 292/2000, *de 30 de noviembre de 2000 del Tribunal Constitucional (recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*).

[91] STC 292/2000 § 8. Article 10(2) of the Spanish Constitution establishes a special interpretative regime for the fundamental rights it enshrines: it asserts the hermeneutical relevance of international treaties ratified by Spain for the interpretation of constitutionally protected rights and freedoms.

[92] Adopted by the UN General Assembly resolution 45/95 of 14 December 1990.

[93] With an argumentation very much indebted to the case law of the German Constitutional Federal Court in its judgment on the Census (Martínez Martínez 2004, p. 239), judgment which had been alluded to by the applicant.

[94] The boundaries were described as corresponding to those of Convention 108, and of the case law of the ECtHR on Article 8 of the ECHR (STC 292/2000 § 9).

[95] STC 292/2000 § 5.

data protection').[96] The Court presented it as having two crucial peculiarities: that its object was not limited to intimate (as in non-public) data, but covered any personal data,[97] and that is was not only about negative prescriptions, but also about the imposition of positive obligations on thirds, with the view of making effective the control by individuals on their personal data.[98] The Court introduced a key nuance in the right's interpretation by affirming that the right encompasses the right to consent to the processing of data irrespective of whether they are processed by computers or not.[99] Thus, the protection of personal data in manual files is to be regarded as part of the constitutional definition of the Spanish right to personal data protection (Guerrero Picó 2006, p. 207). Nonetheless, the right to the protection of personal data was not presented as completely independent, but rather as serving the efficient protection of the *vida privada personal y familiar* ('private and family life'), in the same way as the right to *intimidad* of Article 18(1) of the Constitution.[100]

Greece recognises in its Constitution a right to the protection of personal data, but only since 2001.[101] The Greek Constitution currently states that everybody has the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. It also sets out that the protection of personal data is ensured by an independent authority, constituted and operating as determined by law.[102]

Italy did not recognise a right to the protection of personal data before 2000. A right to the protection of personal data can be said to exist since the adoption of the *Decreto Legislativo 30 giugno 2003, n. 196*,[103] which replaced Law n. 675/1996, and which asserts that everybody has the right to the protection of personal data about them.[104] The right is only recognised in that law, without further constitutional recognition (Lugaresi and Bertazzo 2009, p. 29). However, a provision of the *2003 Decreto Legislativo* brings about some ambiguity about the status of the right to the protection of personal data it establishes, by asserting that the Act's aim is to ensure that personal data processing occurs in compliance with the dignity of the person and fundamental rights and freedoms, in particular *riservatezza* ('privacy'),

[96] The Defensor del Pueblo (the Spanish ombudsman), who had introduced the *recurso de amparo*, referred instead systematically to Article 18(4) of the Spanish Constitution as enshrining a *derecho fundamental a la autodeterminación informativa* ('fundamental right to informational self-determination') (STC 292/2000 § 2).

[97] STC 292/2000 § 6.

[98] Ibid.

[99] Ibid § 7.

[100] STC 292/2000 § 5.

[101] The current Greek Constitution was originally adopted in 1975, and has been revised since several times.

[102] Article 9A of the Greek Constitution (*Constitution of Greece translated by Xenophon Paparrigopoulos and Stavroula Vassilouni* (Hellenic Parliament 2008).

[103] *Decreto Legislativo n. 196/2003, 30 giugno 2003, Codice in materia di protezione dei dati personali* (*GU n.174 del 29-7-2003– Suppl. Ordinario n. 123*).

[104] Article 1(1) of *Decreto Legislativo n. 196/2003, titled* '*Diritto alla protezione dei dati personali*': '*Chiunque ha diritto alla protezione dei dati personali che lo riguardano*'.

identità personale ('personal identity') and the right to the protection of personal data.[105]

Many of the Member States that joined the EU after 2004 included in their Constitutions provisions on the protection of personal data already before 2004. Actually, in many cases they incorporated them already before the adoption of Directive 95/46/EC in 1995.

Hungary revised its Constitution in 1989 (Székely 2008, p. 181), adopting a text that included the right to protection of personal data among the basic rights and freedoms,[106] and which has been expounded by the Hungarian Constitutional Court as establishing that everybody has the right to control the flow of their personal data (Székely 2008, p. 176,178). In January 2012, a new Hungarian Constitution entered into force. The new Constitution prescribes in a single provision that everybody shall have the right to the protection of their personal data, as well as to access and disseminate data of public interest.[107] It also devotes a provision to declare that an independent authority shall supervise the enforcement of both the right to the protection of personal data, and of the right to access data of public interest.[108]

The Slovak Republic adopted a new Constitution in September 1992. Article 19 of the Slovak Constitution enshrines the right to human dignity, personal honour and the protection of good name;[109] the right to protection against unwarranted interference with private and family life,[110] and, finally, the right to protection against the unwarranted collection, publication, or other illicit uses of personal data.[111] The protection of personal data appears additionally in another provision, in the context of the privacy of correspondence and secrecy of messages and written documents.[112]

The Czech Republic also adopted its Constitution in 1992,[113] proclaiming as an integral component of the Czech constitutional system a Charter of Fundamental Rights and Basic Freedoms, formally approved in 1993.[114] The Czech Charter's Article 10 establishes the rights to human dignity, personal honour, respect for good

[105] Article 2(1) of *Decreto Legislativo n. 196/2003: 'Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali'.*

[106] Already in 1977, a measure incorporated in the Civil Code in 1977 the declaration that the processing of data by computerised means shall not violate individual rights.

[107] Article VI (2) of the Hungarian Constitution, adopted on 25 April 2011.

[108] Article VI (3) Hungarian Constitution. This provision generated some criticism. See for instance: *European Parliament Resolution of 5 July 2011 on the Revised Hungarian Constitution*, 5 July 2011, P7_TA(2011)031, Strasbourg.

[109] Article 19(1) of the 1992 Slovak Constitution.

[110] Ibid. Article 19(2).

[111] Ibid. Article 19(3).

[112] Ibid. Article 22.

[113] Adopted on 16 December 1992.

[114] Resolution of the Presidium of the Czech National Council of 16 December 1992 on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic, No. 2/1993 Coll.

reputation and protection of the name;[115] the right to be protected from unauthorised intrusion inter private and family life;[116] and the right to be protected from the unauthorised gathering, public revelation, or any other misuse of personal data.[117]

The Constitution of Lithuania, also adopted in 1992,[118] includes a provision setting out the inviolability of the private life of human beings, and establishing that information concerning the private life of individuals can only be collected upon a justified court order, and in accordance with the law.[119] The constitutional provision is thus not directly concerned with the protection of personal data in the sense of any data related to an identified person, but has allowed the Constitutional Court to interpret it as such (Arenas Ramiro 2007, p. 364).

Poland adopted its current Constitution in 1997,[120] including an innovative provision on private life,[121] which is extensive and detailed (Ordóñez Solís 2011, p. 111). The Article on the protection of personal data, partially inspired by Directive 95/46/EC,[122] prescribes that individuals can be obliged to disclose information concerning them only on the basis of statute,[123] that public authorities shall not process more data than that which is necessary in a democratic state ruled by law,[124] that everyone shall have a right of access to official documents and data collections concerning them,[125] that everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute, and that principles and procedures for collection of information, and for access to such information, shall be specified by statute.[126]

In Estonia, the Constitution, dating from 1992,[127] includes a general provision on the respect of private and family life,[128] but also a specific Article granting to

[115] Article 10(1) Czech Charter.

[116] Ibid. Article 10(2).

[117] Ibid. Article 10(3). In addition, Article 7(1) of the Czech Charter enshrines a right to integrity sometimes translated as right to 'privacy' (Pospíšil and Tichy 2010, p. 5), and Article 13 of the Czech Charter recognises the right to confidentiality of letters or the confidentiality of other papers or records, whether privately kept or sent by post or by some other means, as well as the right to confidentiality of communications.

[118] Constitution of the Republic of Lithuania of 25 October 1992. For an English translation: <http://www3.lrs.lt/home/Konstitucija/Constitution.htm> accessed 20 March 2013.

[119] Article 22 of the Constitution of Lithuania.

[120] Constitution of the Republic of Poland of 2 April 1997. For an English translation, see: <http://www.kprm.gov.pl/english/97.htm> accessed 20 March 2013.

[121] Article 47 of the Polish Constitution. See also: (Safjan 2001, p. 29).

[122] Article 51 of the Polish Constitution.

[123] Ibid. Article 51(1).

[124] Ibid. Article 51(2).

[125] Ibid. Article 51(3).

[126] Ibid. Article 51(5).

[127] Constitution of the Republic of Estonia, adopted on 28 June 1992 (Translation into English by the Estonian Translation and Legislative Support Centre (1996) <http://www.president.ee/en/republic-of-estonia/the-constitution/index.html> accessed 20 March 2013).

[128] Article 26 of Constitution of Estonia.

Estonian citizens[129] the right to access information about themselves 'held in state agencies and local governments and in state and local government archives, pursuant to procedure provided by law' (thus, enshrining a right of access personal data stored in public records).[130]

This panorama might appear to hint that personal data protection is increasingly being treated in European constitutional law as a separate notion (Bygrave 2010, p. 169). In reality, there are still today a number of Member States where personal data protection is not associated to any legal sui generis notion with particular constitutional significance.

6.2.2 Other Approaches

Still today, various EU Member States have not developed a specific legal notion related to the protection of personal data to which link personal data protection laws. Sometimes, the interplay between personal data protection laws and fundamental rights is characterised in terms of the former serving a right to privacy, or a similar notion. Belgium is a prime example of this approach, as it inscribes personal data protection under the right to *vie privée*/ *persoonlijke levensfeer*. Luxembourg is another good example,[131] together with Ireland, where data protection is considered to derive from the right to privacy, recognised as an implicit constitutional right since 1987 (Korff 2002, p. 8).[132]

Since 1991, Bulgaria provides in its Constitution[133] for the protection of privacy and private affairs.[134] The Bulgarian Constitution also proscribes that no one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without their knowledge or despite their express disapproval, except when such actions are permitted by law.[135] Since 2002, the Bulgarian Personal Data Protection Act[136] advances as its purpose to guarantee the inviolability of personality and pri-

[129] As well as citizens of other states and stateless persons who are in Estonia, unless otherwise provided by law (paragraph 4 of Article 44 of the Estonian Constitution).

[130] Third paragraph of Article 44 of the Estonian Constitution. Describing this provision as an element of Estonian constitutional 'privacy framework': (Electronic Privacy Information Center (EPIC) and Privacy International (PI) 2007, p. 421).

[131] See Article 1 of the Coordinated Text of Luxembourg's Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data modified by the Law of 31 July 2006, the Law of 22 December 2006, and the Law of 27 July 2007, which mirrors the wording of Article 1(1) of Directive 95/46/EC.

[132] See also: (Electronic Privacy Information Center (EPIC) and Privacy International (PI) 2007, p. 557).

[133] Constitution of the Republic of Bulgaria, adopted on 13 July 1991.

[134] Article 32(1) Bulgarian Constitution.

[135] Ibid. Article 32(2).

[136] Bulgarian State Gazette No 1/4.1.2002.

vacy.[137] In Romania, the Constitution, adopted in 1991, devotes a provision to the right to *viata intima, familiala si privata* ('intimate, family and private life'),[138] a right the Constitution enshrines[139] together with the freedom of individuals to dispose of themselves.[140] The Romanian law transposing Directive 95/46/EC singles out, among the fundamental rights and freedoms that it aims to guarantee, that right to private life.[141]

The Latvian Constitution was adopted in 1992, even if its section on fundamental human rights was only integrated in 1998.[142] The Constitution includes a provision generally establishing a right to the inviolability of private life, home and correspondence,[143] echoed by the Latvian Personal Data Protection Law when describing its purpose.[144]

In France is still in force the 1978 *loi informatique et libertés*, which, even if its has been amended different times,[145] continues to assert in its opening declaration that *l'informatique* (computers)[146] must not infringe upon human identity, human rights, private life, and individual and public freedoms.[147] France does not recognise the protection of personal data as a separate fundamental right, even though there have been calls for such configuration based on the increased importance of data processing in contemporary society, as well as on the fact that none of currently constitutionally protected French rights and freedoms appears to encompass the whole scope of the envisaged right to personal data protection (Commission nationale de l'informatique et des libertés (CNIL) 2012, p. 23).[148]

---

[137] Article 1(2) of the Personal Data Protetcion Act, which moreover evokes the free flow of personal data.

[138] Ibid. Article 26.

[139] Ibid. Article 26(1).

[140] Ibid. Article 26(2).

[141] See Article 1(1) of Romanian Law No. 677/2001 of 21 of November 2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.

[142] For an English translation of the Constitution of the Republic of Latvia (with amendments up to 8.4.2009), see: <http://www.satv.tiesa.gov.lv/?lang=2&mid=8> accessed 20 March 2013.

[143] Article 96 of the Latvian Constitution.

[144] According to its first Article, the purpose of the law is to protect the fundamental human rights and freedoms of natural persons, in particular the inviolability of private life, regarding the processing of data of natural persons.

[145] In particular, in 2004 to transpose Directive 95/46/EC.

[146] Or, according to the English translation published by the CNIL, 'information technology' (Act N 78–17 Amended by the act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data (last update: Ordinance No. 2011–1012 dated 24/08/2011) <http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf> accessed 20 March 2013). The document asserts that the CNIL decided not to translate the original titles of French institutions or procedures 'when their translation may be misleading', and presents as an instance of such potentially misleading titles the very name of the CNIL (ibid. ii).

[147] Article 1 of French *loi informatique et libertés:* '*(l'informatique) ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*'.

[148] Observing however that the French *Conseil constitutionnel* refers more and more often to the protection of personal data: (Desgens-Pasanau 2012, p. 7).

Still, some European data protection statutes make no reference at all to the safeguarding of privacy (Bygrave 2002, p. 37). Sweden, for instance, frames the protection of personal data under the protection of 'personality', or the protection of 'personal integrity'.[149] Additionally, some national statutes do not contain any clauses formally specifying a particular interest or value as values or interests that they intend to serve (Bygrave 2002, p. 37). Denmark, despite having a data protection statute since 1978, lacks a firm constitutional basis for the notion of personal data protection, or even for the notions of 'privacy' or 'private life'.[150] The Danish Constitution focuses on the protection of the inviolability of the home, and of privacy of 'correspondence and other papers'.[151] The Act on the Processing of Personal Data with which Denmark transposed Directive 95/46/EC in 2000, and which has been repeatedly amended since, does not portray itself as implementing any fundamental right in particular.[152]

This overview shows that it is extremely difficult to assert the existence of a common constitutional tradition in EU Member States in relation to the right to the protection of personal data. It was even more difficult to maintain there existed such common tradition before the year 2000 (Tiberi 2007, p. 375).

6.3 Appearance of Data Protection Among EU Fundamental Rights

For many decades, EU institutions discussed two possible paths to reinforce their formal commitment to fundamental rights: either EU's accession to the ECHR, suggested by the European Commission already in 1979, even if with very little success, or EU's writing of a new rights' catalogue, an approach supported by some already in the 1980s.

[149] Section 1 of Sweden's Personal Data Act of 1998 (*Personuppgiftslagen*, SFS 1998:204). See: (Bygrave 2002, p. 37). See also: (Korff 2002, p. 8).

[150] The European Convention on Human Rights is directly applicable in Denmark, but it is not accorded special status (Korff 2002, p. 9).

[151] Article 72 of the Danish Constitution stipulates that the confiscation and examination of letters and other papers, as well the interception of postal, telegraph and telephone communications, cannot be done without a judicial order (Prakke and Kortmann 2004, p. 163).

[152] Compiled version of the Act on Processing of Personal Data Act No. 429 of 31 May 2000 as amended by Section 7 of Act No. 280 of 25 April 2001, Section 6 of Act No. 552 of 24 June 2005, Section 2 of Act No. 519 of 6 June 2007, Section 1 of Act No. 188 of 18 March 2009, Section 2 of Act No. 503 of 12 June 2009, Section 2 of Act No. 422 of 10 May 2011 and Section 1 of Act No. 1245 of 18 December 2012 (English version translated for the Danish Data Protection Agency: <http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/> accessed 10 March 2013).

6.3.1 First Lists

During the 1980s, different Members of the European Parliament attempted to draw up new lists of European fundamental rights. Vivid discussions emerged in particular as a Committee on Institutional Affairs, set up at the European Parliament in 1981, decided to write down a draft Treaty establishing the European Union,[153] which was branded as a future Constitution for Europe. Altiero Spinelli, who had been previously at the Commission but had since been elected to the European Parliament, coordinated the work of six rapporteurs addressing each a specific subject related to the preparation of this Constitution. Karel De Gucht was named rapporteur on the law of the Union.[154] In this context, De Gucht considered pertinent to elaborate a new list of rights, and to have this list integrated into the text of the draft Constitution. Spinelli, however, opposed the idea, regarding it as extremely challenging, and ultimately useless (Spinelli 1992, p. 796, 1067).

De Gucht eventually argued, in his 1983 official contribution as rapporteur on EU's legal structure, that fundamental rights protection shall be a vital task for the EU, and that, for this purpose, the upcoming Treaty imperatively needed to 'contain a list of civil and political rights based primarily on the (ECHR), the common principles contained in the Member States' Constitutions and the United Nations International Covenant on Civil and Political Rights'.[155] Still in 1983, two Members of the European Parliament introduced a motion for resolution precisely aimed at incorporating at Treaty level an explicit enumeration of rights.[156] They presented a draft for a Constitution listing constitutionally protected rights,[157] among which they included a right to 'inviolability of privacy'.[158] The Plenary of the European Parliament, however, rejected their suggestion to include a list of rights in the draft Treaty.

The European Parliament finally adopted in 1984 a draft Treaty on European Union,[159] also known as the Spinelli draft, which merely asserted that the EU 'shall protect the dignity of the individual and grant every person coming within its jurisdiction the fundamental rights and freedoms derived in particular from the common

[153] Committee on Institutional Affairs of the European Parliament, *Working Document containing the "White Paper" on the state of fundamental rights in the European Community* (*Rapporteur: Mr K. de Gucht*) PE 115.274, July 1987, 16.

[154] Ibid.

[155] European Parliament, *Report drawn up on behalf of the Committee on Institutional Affairs concerning the substance of the preliminary draft Treaty establishing the European Union, Part B: Explanatory Statement*, Document 1-575/83/B, 15.7.1983, 8.

[156] European Parliament, *Motion for a Resolution tabled by Mr Luster and Mr Pfennig jointly*, Document 1-653/83/rev., 26.9.1983.

[157] Chapter II of the draft Constitution.

[158] Article 6, which read: '1. The inviolability of the home and the privacy of post and telecommunications shall be guaranteed. 2. Restrictions shall only be permissible by virtue of this constitution and the constitutions of the States of the Union' (Document 1-653/83/rev., 14).

[159] On 14 February 1984.

principles of the Constitutions of the Member States and from the (ECHR)'.[160] As a gesture towards those who had advocated in favour of the inclusion in the draft Treaty of a list of rights, the text gave the EU 5 years to take a decision on the possible accession of the EU to the ECHR, as well as to 'adopt its own declaration on fundamental rights'.[161]

Shortly after the adoption of this draft for a Constitution, new calls for the elaboration of a list of rights resurfaced at the European Parliament.[162] Its Committee on Institutional Affairs decided to keep actively exploring the issue, and appointed[163] Karel De Gucht as rapporteur to deal with the task, on the basis of the work he had already carried out.[164]

By 1987, De Gucht completed a White Paper[165] reviewing the fundamental rights protected by Community law. The White Paper identified the 'protection of private life' as one of them. It described its content by alluding to the case law of the ECJ, but also to various resolutions of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing,[166] and, thus, advanced data processing issues as integral to the protection of private life. Following a discussion of the White Paper by the Committee on Institutional Affairs in 1988, De Gucht prepared a draft proposal for resolution to be submitted to the Plenary.[167]

Based on that text, the European Parliament adopted on 12 April 1989 a Declaration of Fundamental Rights and Freedoms[168] constituting the first comprehensive catalogue of rights ever endorsed by an EU institution. Although it lacked any legally binding force, the Declaration emphasised that the European Parliament was 'determined to achieve a basic Community instrument with a binding legal character guaranteeing fundamental rights'.[169] The rights it listed were portrayed as deriving

[160] Article 4(1) of the 1984 draft Treaty establishing the European Union.

[161] Ibid. Article 4(3).

[162] On 26 July 1984, a motion for a resolution was tabled by Mr Luster and Mr Pfennig to supplement the draft Treaty establishing the European Union was referred to the Committee on Institutional Affairs.

[163] In October 1984.

[164] PE 115.274, 17.

[165] PE 115.274.

[166] Ibid. 223.

[167] *Report drawn up on behalf of the Committee on Institutional Affairs on the Declaration of Fundamental rights and freedoms (General rapporteur: Mr Karel De Gucht),* PE 127.111/fin, 20.3.1989. The draft of the Declaration was prepared at a meeting in Knokke, where the rapporteur was assisted by Professors Meinhard Hilf (Universität Bielefeld), Joseph H. H. Weiler (University of Michigan, and Jean-Paul Jacqué (Université de Strasbourg) (ibid. 3), the later being particularly familiar with personal data protection, a subject on which he had published (see, for instance: (Jacqué 1980)).

[168] Resolution of the European Parliament adopting the Declaration of fundamental rights and freedoms [1989] OJ C120/51.

[169] Preamble, paragraph G.

from the EC Treaties, the constitutional traditions common to the Member States, the ECHR, and the case law of the ECJ.

The 1989 Declaration of Fundamental Rights and Freedoms comprised three provisions somehow related to the protection of personal data. First, it devoted an Article to 'Privacy',[170] establishing that everyone shall have the right to respect and protection for their identity, and respect for privacy and family life, reputation, home and private correspondence—a provision that thus disregarded the expression private life in favour of the term privacy. Second, the 1989 Declaration put forward another Article, titled 'Right of access to information',[171] establishing that '(e)veryone shall be guaranteed the right of access and the right to corrections to administrative documents *and data concerning them*'.[172] Third, an Article on 'Freedom of association' foresaw that no one shall 'in their private life be required to disclose their membership of any association which is not illegal'.[173]

In 1994, the European Parliament voted another draft Constitution, including this time a rights catalogue,[174] based on what was known as the Herman Report.[175] The new list, titled 'Human rights guaranteed in the Union', introduced a revised version of the Article of the 1989 Declaration on 'privacy', now expanded with a reference to judicial authorisation as a condition for surveillance by public authorities.[176] The list also maintained the previous wording of the Article on 'Right of access to information',[177] but obliterated the prescription of disclosure of membership of legal associations in its Article on 'Freedom of association'.[178]

The 1992 Maastricht Treaty foresaw the celebration in 1996 of an Intergovernmental Conference to consider further changes in the Treaties, to bring the EU up to date, and to prepare it for the next enlargement—an Intergovernmental Conference that eventually led to the Amsterdam Treaty. To prepare it, the European Council set up in 1994 a special Reflection Group.[179] Its members requested the Secretariat of the Council to provide a summary of the rights and principles included in the con-

[170] Article 6 of the 1989 Declaration of fundamental rights and freedoms.

[171] Ibid. Article 18.

[172] Emphasis added.

[173] Ibid. Article 11.

[174] Resolution of the European Parliament on the Constitution of the European Union (Herman report) of 10.02.1994 (A3-0064/94) [1994] OJ C61/155. Work on this new draft had started in 1990. By letter of 23 January 1990, the Committee on Institutional Affairs had requested authorization to draw up a report on the European Constitution (European Parliament, *Second Report of the Committee on Institutional Affairs on the Constitution of the European Union (Rapporteur: Mr Fernand Herman)*, A3-0064/94, PE 203.601, 9.2.1994, 3).

[175] Ibid.

[176] Article 6(c) of Title VIII: 'Surveillance by public authorities of individuals and organizations may only take place if duly authorized by a competent judicial authority' (1994 Resolution on the Constitution of the European Union, 166). See also: PE 203.601, 36.

[177] Article 15 of Title VIII Resolution on the Constitution 1994.

[178] Ibid. Article 9 of Title VIII.

[179] The Corfu European Council of 24 and 25 June 1994.

stitutions of the Member States, leading to the elaboration of a note[180] that stressed the differences in recognition of rights and principles across Member States, concerning their level in the hierarchy of norms, but also their content, beneficiaries, and judicial guarantee.[181] The note classified national constitutional provisions on the protection of personal data as referring to the right to privacy,[182] and drew the attention on the existence of a right to information, in the sense of a right to access to documents held by public authorities, in five of the then fifteen Member States: Belgium, Spain, the Netherlands, Finland, and Sweden.

The Reflection Group published in 1995 a report called *A Strategy for Europe* discussing the main challenges to be addressed by the 1996 Intergovernmental Conference. The report notably observed that, on the basis of its inquiries, it was clear that some favoured the inclusion in the Treaties of a general principle of access to documents of the Union,[183] in the form of a right of access to information.[184] There was no particular mention of the right to the protection of personal data.

In 1998, a Committee of the European Parliament[185] publicly referred to the right to the protection of personal data as a fundamental right, but did so almost incidentally—in the course of its annual review of respect of human rights in EU.[186]

6.3.2 The Comité des Sages

At the beginning of the 1990s, EU institutions were particularly concerned with the status in EU law of fundamental social rights. A Community Charter of the Fundamental Social Rights of Workers[187] had been adopted in 1989 by a declaration of all Member States (with the exception of the United Kingdom), but the exact relationship between this Charter and EU law was unclear. In the context of the preparation of the 1996 Intergovernmental Conference, the European Commission appointed a special Committee, known as Comité des Sages, to explore the future of that Community Charter in connection with the upcoming Treaty reform.

The Comité des Sages appointed by the Commission accepted the task, but decided to expand its remit, and to discuss more widely the relationship between EU law and social and civic rights. In 1996, the Comité des Sages published a final report

[180] Private Office of the General Secretariat of the Council of the European Union, *Note for the Reflection Group on the Principles and rights included in the constitutions of the Member States of the European Union*, SN 512/95 (REFLEX 13), Brussels, 6.10.1995.

[181] Ibid. 1.

[182] Ibid. 3 (in reference to Austria, for instance).

[183] Reflection Group, *Reflection Group Report: A Strategy for Europe*, DOC/95/8 (1995) paragraph 67.

[184] Ibid 6.

[185] The Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee).

[186] *Annual Report of 2 December 1998 on respect for human rights in the European Union*, PE 228.192/fin (1997) para 23. See also: (Coudray 2010, p. 296).

[187] Community Charter of Fundamental Social Rights of Workers, 9 December 1989.

recommending the enshrinement in the Treaties of a basic set of rights, in the form of a bill (Comité des Sages chaired by Maria de Lourdes Pintasilgo 1996). The supported bill should not merely reflect existing rights, but actively '(n)urture the emergence of a new generation of civic and social rights, reflecting technological change, enhanced awareness of the environment and demographic change' (1996, p. 9).

The Comité des Sages argued that 'new technologies are creating many problems in terms of fundamental rights: thus the information society may threaten individual privacy' (1996, p. 41). Taking the view that 'the list of fundamental rights is not unchangeable', the Comité des Sages maintained it was necessary to stimulate the recognition of new rights in particular 'because technological progress is creating threats to individuals' (1996, pp. 15–16).

6.3.3 The Amsterdam Treaty

The Treaty of Amsterdam, signed on 2 October 1997, did not bring about the suggested inclusion in the Treaties of a specific EU list of rights (Poiares Maduro 1999, p. 461). Regarding social rights, was incorporated an allusion to the fundamental social rights set out in the European Social Charter signed at Turin on 18 October 1961 and in the 1989 Community Charter of the Fundamental Social Rights of Workers (Poiares Maduro 1999, p. 461). In relation to personal data protection, the Amsterdam Treaty incorporated Article 286 of the EC Treaty, establishing that, starting from 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to Community institutions and bodies,[188] and that before that date shall be established an independent supervisory body to monitor the application of such acts in that context.[189]

The Amsterdam Treaty integrated among EU objectives the notion of openness, advancing transparency as one of the paths to restore the EU democratic deficit (Oreja Aguirre and Fonseca Morillo 1998, p. 209). It also incorporated into the Treaties a new fundamental right: the right of access to the documents of EU institutions (Oreja Aguirre and Fonseca Morillo 1998, p. 212). In 1992, as the European Council adopted the Treaty of Maastricht, a declaration had been published stressing the importance of the right of access to documents, linking this right to EU institutions' democratic nature (Öberg 1998, p. 2). In 1993, the European Council invited the Council and the Commission to work in this direction,[190] leading to the adoption of a Code of Conduct[191] concerning public access to Council and Commission documents (Öberg 1998, p. 3) and the measures to implement it both in

[188] Article 286(1) of the EC Treaty.

[189] Article 286(2) of the EC Treaty. See Chap. 5, Sect. 5.2.3.1, of this book.

[190] At the meeting held in Copenhagen on 22 June 1993.

[191] Code of Conduct (93/730/EC) of 6 December 1993, concerning public access to Council and Commission documents [1993] OJ L340/l.

the Council[192] and in the Commission.[193] The two implementing decisions foresaw exemptions to documents' disclosure when such disclosure could undermine 'the protection of the individual and of privacy'.[194]

The accession to the EU in 1995 of Sweden (along with Finland and Austria) further increased the pressure towards open government (Oreja Aguirre and Fonseca Morillo 1998, p. 210). Sweden, which regards the principle the openness as one of the foundational principles of its democratic order, made a declaration before its accession reminding EU Member States of the importance it attached to such *offentlighetsprincip* (Steele 2002, pp. 19–20). At the end of 1995, the Swedish Permanent Representation to the EU organised in Brussels a Seminar on *Openness and Transparency in the European Union*, announcing a proposal to be submitted to the 1996 Intergovernmental Conference (European Commission 1995). In 1996, the Swedish Government published an official note on openness,[195] recalling its attachment to the principle of public access to official documents, and observing that it nonetheless needed to be 'coupled with rules on secrecy to protect specific confidential interests, such as security reasons, public safety, relations to third countries, business and financial secrets and the protection of individuals *and of privacy*[196]' (Swedish Ministry of Justice 1996a, p. 3). During the 1996 Intergovernmental Conference, Sweden, but also Denmark, Finland and the Netherlands, firmly pushed for the insertion in the Treaties of the principle of public access to documents held by EU institutions (Öberg 1998, p. 11).

6.3.4 The Expert Group on Fundamental Rights

After the adoption of the Treaty of Amsterdam, and to follow up the work of the Comité des Sages, the European Commission entrusted a new Group of Experts to further analyse the possibility of explicitly recognising in EU law a list of fundamental rights. The European Commission pointed to some questions as particularly worthy of attention, such as the possibility to include, in any future catalogue, new rights mirroring the challenges of information society (Expert Group on Fundamental Rights 1999, p. 6).

Spiros Simitis chaired the Expert Group. Simitis, formally credited then as Director of the Research Centre for Data Protection of the University of Frankfurt (1999, p. 18), had been one of the drafters of pioneering German data protection laws, as well as Data Protection Commissioner of the Land of Hesse from 1975 to

[192] Council Decision 93/731/EC of 20 December 1993 on public access to Council documents [1993] OJ L340/43.

[193] Commission Decision of 8 February 1994 on public access to Commission documents (94/90/ECSC, EC, Euratom) [1994] OJ L46/58.

[194] Article 4(1) of Council Decision 93/731/EC.

[195] It also submitted a Working Document on the subject to the 1996 Intergovernmental Conference: (Swedish Ministry of Justice 1996b).

[196] Emphasis added.

1991, data protection expert at the Council of Europe at the beginning of the 1980s, and consultant for the European Commission since 1988 in matters of data protection.

The Expert Group published a final report in 1999, describing the state of fundamental rights protection in EU law as unsatisfactory. It notably underlined that there had been manifest attempts to limit the influence of fundamental rights in EU's second and third pillar, bringing forward as a paradigmatic example of this problem the protection of personal data. In this sense, the Expert Group noted that although Directive 95/46/EC had 'pointed to the direct link between data protection and fundamental rights', generally accepted data protection principles appeared to be to a large extent abandoned in the third pillar (1999, p. 8). Action was needed, the Expert Group argued, to reinforce fundamental rights protection throughout all activities of EU institutions and bodies (1999,p. 8).

The Expert Group presented a series of recommendations for the explicit recognition of fundamental rights in the EU, calling for the acknowledgement of all rights provided in Articles 2–13 of the ECHR, but also for the addition of some clauses 'detailing and complementing the ECHR', one of 'the most obvious' examples of a necessary addition being 'the right to determine the use of personal data' (1999, p. 2, 8, 17). The Expert Group also stressed that the identification of fundamental rights needed to be understood as a process, resulting in 'a reformulation of fundamental rights adapted to the experiences and exigencies of the European Union', and to remain an open process (1999, p. 17).

6.4 The EU Charter of Fundamental Rights

The European Council, meeting in Cologne in June 1999, decided that a 'Charter of fundamental rights of the EU' should be adopted,[197] in order to make the importance of existing fundamental rights more visible to EU citizens, and to consolidate them at EU level.[198] The elaboration of the Charter of Fundamental Rights was marked by a tension between the Convention's task to render more visible already existing rights, and the possibility (and for some, the opportunity) to innovate within this mandate. This friction stems, allegedly, from the ambiguities at the core of any codification process: to render more visible existing rights, it might be necessary to identify rights that are not particularly visible, and there might be only a thin line between an invisible right and a non-existing right. Fundamental rights, moreover, have sometimes been described as having an inherent *vis expansiva* (García Roca and Fernández Sánchez 2009, p. xxviii).

[197] See: European Council Decision on the drawing up of a Charter of Fundamental Rights of the European Union, in Annex IV to the Presidency Conclusions, 3 and 4 June 1999.

[198] Paragraph 44 of European Council Presidency Conclusions of the Cologne European Council of 3 and 4 June 1999.

During the drafting stage, some Member States, and notably, the United Kingdom, insisted on the idea the Convention has not been required to create any new rights (Braibant 2001, p. 47). Some Convention participants, nonetheless, were attached to the flexibility allowed by this kind of codifying exercises, and pointed out the convenience of including in the upcoming rights catalogue any important 'modern' rights, be it in relation to bioethics, the environment, consumer rights, or computers (Braibant 2001, p. 47).

Already in September 1999, the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (generally known as the Article 29 Working Party), composed of representatives of the data protection authorities of Member States, manifested its support for the inclusion in the upcoming catalogue of a right to the protection of personal data (Article 29 Data Protection Working Party 1999, p. 3). The Working Party issued an ad hoc Recommendation welcoming the initiative to draw up a EU bill of rights, and remarked that some European countries had already incorporated 'fundamental rights on data protection' into their constitutions, while in others these rights had acquired constitutional status through case law (Article 29 Data Protection Working Party 1999, p. 2). The Article 29 Working Party also asserted that the ECtHR[199] had in its case law 'developed and defined a fundamental right based on various human rights which relate to the protection of personal data' (1999, p. 2).

The European Parliament equally welcomed the decision of the Cologne European Council to launch the drawing up of a Charter of Fundamental Rights. In a Resolution of 16 September 1999, the European Parliament highlighted 'the need for an open and innovative approach to (…) the nature of the rights to be featured in it'.[200] Later, it issued a new Resolution[201] underlining that the Charter should be 'innovative in nature' and ensure legal protection in respect of new threats to fundamental rights, for example in the field of information technology.[202]

6.4.1 Drafting

The European Council[203] formally entrusted the Charter's drafting to a special body composed of representatives of the heads of State and Government, the President

[199] Together with the European Commission of Human Rights.

[200] Resolution of the European Parliament on the establishment of the Charter of Fundamental Rights, of 16 September 1999 (B5-0110/1999) [1999] OJ C54/93 paragraph 3.

[201] Resolution of the European Parliament of 16 March 2000 on respect for human rights in the European Union (1998–1999) (11350/1999–C5-0265/1999–1999/2001(INI)), A5-0050/2000 [2000] OJ C377/335 paragraph 7(a).

[202] Ibid. paragraph 7(h).

[203] The Cologne European Council had specified that 'a draft of such a Charter of Fundamental Rights of the European Union should be elaborated by a body composed of representatives of the Heads of State and Government and of the President of the Commission as well as of members of the European Parliament and national parliaments'. In addition: 'Representatives of the European

of the European Commission, Members of the European Parliament[204] and national Members of Parliament.[205] The body decided to call itself 'the Convention'.[206]

The Convention was chaired by the German Roman Herzog, former President of the Federal Republic of Germany and of the Federal Constitutional Court of Germany, and a professor of constitutional law (Pati 2012, p. 243). He was thus peculiarly familiar with the German Federal Constitutional Court's case law on the right to informational self-determination. Another participant to the Convention was the French Guy Braibant,[207] whose links with the regulation of data processing can be traced back to his indirect influence of the drafting of the 1978 law on *informatique et libertés*,[208] and who in 1998 had prepared a report on Directive 95/46/EC for the French government (Braibant 1998). He took part in the Convention representing France. One of the two representatives of the Spanish Parliament was Jordi Solé Tura, who had actively contributed to the drafting process of the 1978 Spanish Constitution, and concretely to the discussions on the wording on the provision later to be known as establishing a fundamental right to the protection of personal data.[209] And, officially representing Italy, there was Stefano Rodotà,[210] who had notably been member of the Expert Group set up in 1978 to draft the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Rodotà was at the time Chairman of the Italian data protection authority, as well as member of the Article 29 Working Party that had already expressed its full support for the inclusion in the Charter of a fundamental right to the protection of personal data.[211]

Rodotà was also, at the same time, one of the twelve members of the European Group on Ethics in Science and New Technologies, a body providing advice to the European Commission since 1991. Following a personal request by the President of the European Commission, Romano Prodi, the advisory group produced a report on fundamental rights and technological innovation that was forwarded

---

Court of Justice should participate as observers. Representatives of the Economic and Social Committee, the Committee of the Regions and social groups as well as experts should be invited to give their views. Secretariat services should be provided by the General Secretariat of the Council' (see: European Council, Presidency Conclusions of the Cologne European Council of 3 and 4 June 1999, and in particular 'Annex IV: European Council Decision on the Drawing Up of a Charter of Fundamental Rights of the European Union').

[204] Concretely, there were: fifteen representatives of the Heads of State and Government, 30 representatives of the national parliaments, sixteen representatives of the European Parliament, and one representative of the Commission.

[205] On 15 and 16 October in Tampere, Finland, the European Council laid down the exact composition and working methods of the body responsible for drawing up the draft Charter.

[206] During its first meeting on 17 December 1999.

[207] Participating with the status of member of the Convention Bureau.

[208] See Chap. 3, Sect. 3.1.4, of this book.

[209] Article 18(4) Spanish Constitution. See Chap. 3, Sect. 3.2.3, of this book.

[210] Describing the presence of Braibant and Rodotà as favourable for the recognition of a right to the protection of personal data: (Coudray 2010, p. 297).

[211] On the strategic position of Rodotà, see also: (Article 29 Data Protection Working Party 2002, p. 23).

to the Convention.[212] In this report, the European Group on Ethics in Science and New Technologies defended the insertion in the Charter of a detailed Article on the protection of personal data, identifying as key data protection principles: data confidentiality, the right to determine which data are processed, by whom, and for what purposes, and the rights to access, correction or erasure, and proscribing the use of surveillance technologies aiming at or resulting in a violation of rights or freedoms.[213]

As the Convention started to discuss the drafting of the Charter, it was uncertain whether the final text would generate enough consensus among Member States in order to be adopted as a legally binding text (Dutheil de la Rochère 2003, p. 230). The participants, nevertheless, accepted Herzog's suggestion to work on the draft *as if* it might 1 day acquire legally binding force (Dutheil de la Rochère 2003, p. 230).

At the beginning of January 2000 was submitted to the Convention a discussion draft elaborated by a German representative, Jürgen Meyer, based on the European Parliament's Declaration of fundamental rights and freedoms of 1989.[214] The draft gave particular prominence to data protection, to which it devoted a special Article[215] with two paragraphs, reading as follows: 'Everyone shall have the right to determine for himself the disclosure and use of his personal data and to obtain information on their storage provided that this right does not conflict with the rights of third persons', and '(r)estrictions shall be admissible by law only in the dominant general interest".[216]

A tentative list of rights to be considered by the Convention, distributed by the Convention's Bureau (called Praesidium) by the end of January,[217] also took as major source of inspiration the 1989 Declaration of fundamental rights and freedoms of the European Parliament, and invited to reflect on the possibility to recognise a

[212] European Group on Ethics in Science and New Technologies, 'Citizens rights and new technologies: Report of the on the Charter on Fundamental Rights related to technological innovation requested by President Prodi on February 3, 2000', 23.5.2000, Brussels, reproduced in: *Draft Charter of Fundamental Rights of the European Union*, CHARTE 4370/00 CONTRIB 233, Brussels, 15.6.2000.

[213] The proposed Article read: '15.1. Everyone has the right to protection for their personal data. 15.2. In the field of data protection, the following principles in particular must be respected: —respect for confidentiality of personal individual data;—right to determine which of one's own data are processed, by whom and for what purposes;—right to have access to one's own data and to correct or delete them. 15.3. No person shall be subject to surveillance technologies, which aim at or result in the violation of their rights or liberties' (CHARTE 4370/00 CONTRIB 233, 26).

[214] *Cover Note: Subject: Draft Charter of Fundamental Rights of the European Union*, CHARTE 4102/00, CONTRIB 2 (OR. Fr.), Brussels, 6.1.2000.

[215] Article 6, preceding an Article 7 on privacy.

[216] Ibid. 4.

[217] *Presidency Note: Subject: Draft list of fundamental rights,* CHARTE 4112/2/00 REV 2, BODY 4 (Or. f.) Brussels, 27.1.2000.

right to respect to private and family life encompassing a right to privacy,[218] and, separately, an additional right to data protection.[219]

The members of the Convention soon agreed on the appropriateness of including in the Charter at least a reference to the protection of personal data (Martín y Pérez de Nanclares 2008, p. 227), initially always referred to as 'data protection'. An Article[220] on 'data protection' appeared in a draft of February 2000,[221] in this form: 'Data protection: Every natural person shall have a right to protection for his personal data'.[222] The comments accompanying this provision mentioned as its sources Article 286 of the EC Treaty and the EC Directives on data protection (and, indirectly, Convention 108), and observed that the proposed Article could apply to the protection of data in manual files. The accompanying comments also claimed that '(i)n any case, data protection is an aspect of respect for privacy',[223] referring to the 1989 Declaration of the European Parliament as a proof of that conception. The same draft provided however also an alternative, longer wording for the Article: '(r)espect for the rights and freedoms laid down by this Charter, and in particular the right to privacy, shall be guaranteed with regard to the processing, by whatever means, of any information concerning an identified or identifiable natural person. The information must be processed fairly and for specified purposes, and subject to the data subject's consent or to any other legitimate basis specified by law'.[224] The possibility to include a reference to the need to foresee control of compliance by an independent body was also put on the table.[225]

In May 2000, another draft formulation for an Article titled 'data protection'[226] saw the light. It read: 'Everyone has the right to determine for himself whether his personal data may be disclosed and how they may be used'.[227] The accompanying

[218] A construction influenced by, according to the document, the 1989 Declaration of the European Parliament, and Article 8 of the ECHR (ibid. 5). The French version, which is the official original, alludes to a right to *respect de la vie privée* that would include a right to *intimité.* The German mentions a *Achtung des Privatlebens* that would include a *Recht auf Privatsphäre*.

[219] A construction influenced by, according to the document, the 1989 Declaration of the European Parliament, and Article 286 of the EC Treaty (ibid. 4).

[220] Numbered Article 15.

[221] *Note from the Praesidium, Subject: Draft Charter of Fundamental Rights of the European Union—Proposed Articles (Articles 10–19)*, CHARTE 4137/00, CONVENT 8 (OR. fr), Brussels, 24.2.2000.

[222] Ibid. 5.

[223] Ibid. In the French original: '*(e)n tout état de cause, la protection des données est un élément du respect de la vie privée*'.

[224] CHARTE 4137/00, CONVENT 8, 5.

[225] Ibid.

[226] Renumbered as Article 19.

[227] *Draft Charter of Fundamental Rights of the European Union – New proposal for Articles 1–30 (Civil and political rights and citizens' rights*), CHARTE 4284/00, CONVENT 28(OR. fr), Brussels, 5.5.2000, 19.

comments reasserted that '(i)n any case, data protection is an aspect of respect for privacy'.[228]

Eventually some Convention members suggested to delete the discussed Article on data protection, and to incorporate instead a reference to data protection under the right to respect for private life.[229] A Dutch representative, Frits Korthals Altes,[230] argued that the envisaged Article was 'too broad in view of (recent) legislation in force in the Member States on data protection'.[231] A representative of the Swedish Government, Daniel Tarschys,[232] argued in favour of the provision, but advised that its heading should be changed into 'personal data protection'.[233] A number of proposed amendments called for a more detailed clarification of the right's content[234] and limits.[235] Rodotà co-authored an amendment overtly connecting data protection to the protection of identity, human dignity and to something that the English translations refer to as confidentiality, but might have been originally *riservatezza*.[236]

The provision surfaced in its almost definitive version by July 2000. Titled 'personal data protection', and numbered Article 8, it established: 'Everyone has the right to the protection of personal data concerning him'. Such data must be processed fairly for specified purposes on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent

[228] Ibid. The English translation also uses the word privacy in the Article corresponding to the right to respect for private life: 'Article 12. Respect for private life: Everyone has the right to respect for his privacy, his honour and his reputation, his home and the confidentiality of his correspondence and communications' (ibid. 13).

[229] *Praesidium Note, Subject: Draft Charter of Fundamental Rights of the European Union—Amendments submitted by the members of the Convention regarding civil and political rights and citizens' rights (Reference document: CHARTE 4284/00 CONVENT 28 (REV 1 in French only)*, (OR. multilingual), CHARTE 4332/00, CONVENT 35, Brussels, 25.5.2000 (see, in particular, 448). A German member was concerned with the use, in the German drafts distributed, of the word Privatleben; he and other German-speaking members supported that the word be replaced with Privatsphäre, regarded as having a broader meaning (ibid. 281); see also, in this sense, Amendment 216 introduced by Jürgen Gnauck (ibid. 284). Although initial drafts referred to a right to privacy, the term was eventually changed into 'respect for private life', to enhance coherence with the ECHR (see draft amendments to document CHARTE 4149/00 CONVENT 13 by Lord Goldsmith, QC, Personal Representative of the Government of the United Kingdom: Cover Note on Draft Charter of Fundamental Rights of the European Union, CHARTE 4179/00, CONTRIB 62, Brussels, 28.3.2000).

[230] Lawyer, senator and former Justice Minister.

[231] CHARTE 4332/00, CONVENT 35, 288.

[232] Professor of political science.

[233] Ibid. 447.

[234] Such as Amendments 371 (ibid. 456), 372 (ibid. 462), 374 (ibid. 464), 376 (ibid. 466), or 378 (ibid. 468).

[235] Such as Amendments 360 (ibid. 450), 362 (ibid. 452), 363 (ibid. 453), or 377 (ibid. 467). See also, on the amendments proposed: (Bernsdorff 2003, p. 159).

[236] Amendment 373 (CHARTE 4332/00, CONVENT 35, 463).

authority'.[237] Later, to improve its readability, the Presidency divided the text of Article 8 into three separate paragraphs (Bernsdorff 2003, p. 159).

The comments elaborated under the authority of the Praesidium accompanying the Charter, by then formally renamed 'explanations' and later made public for information purposes, specified that this Article was based on Article 286 of the EC Treaty, on Directive 95/46/EC, on Article 8 of the ECHR, and on Convention 108. They also clarified that the right to the protection of personal data could be limited under the conditions set out in the draft Charter's Article 50, which was titled 'scope of guaranteed rights' and provided horizontal guidance on right's limitations.[238] The assertion according to which data protection was an element of privacy disappeared.

The draft of the Charter was officially concluded on 2 October 2000. The European Parliament assented to the draft on 14 November 2000, and the Charter of Fundamental Rights of the EU was formally proclaimed by the leaders of EU institutions on 7 December 2000 in Nice.[239]

6.4.2 Personal Data Protection in the EU Charter

The preamble to the EU Charter declares that it 'reaffirms' rights 'as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Community and by the Council of Europe, and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights'.[240] It also notes, however, that it aims at strengthening the protection of fundamental rights 'in the light of changes in society, social progress and scientific and technological developments'.[241]

The Charter is divided into seven Chapters: six Chapters list rights and principles (grouped according to the basic notions of dignity, freedoms, equality, solidarity, citizens' rights and justice), and a seventh one covers general provisions.

---

[237] *Presidency Note: Subject: Draft Charter of Fundamental Rights of the European Union—Complete text of the Charter proposed by the Praesidium*, CHARTE 4422/00, CONVENT 45 (OR. Fr), Brussels, 28.7.2000, 4. By then, the English translation of the provision of the right to respect for private life had also been amended (ibid.).

[238] *Presidency Note, Subject: Draft Charter of Fundamental Rights of the European Union—Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4422/00 CONVENT 45*, CHARTE 4423/00, CONVENT 46 (OR. Fr.), Brussels, 31.7.2000.

[239] Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

[240] Ibid.

[241] Linking this sentence with the protection of personal data in Article 8 of the EU Charter: (Rodotà 2010, p. 57).

6.4.2.1 Locating Personal Data Protection in the EU Charter

The Charter includes two Articles directly relevant for the protection of personal data, both appearing in Chap. II, called 'Freedoms': Article 7, on the right to respect for private and family life, [242] and Article 8, on the right to the protection of personal data. Article 7 on the right to respect for private and family life must be regarded relevant to the extent that it mirrors Article 8 of the ECHR, and that this Article's scope has been outlined by the ECtHR as concerned with the processing of information about individuals. Article 8 of the Charter is openly specifically devoted the protection of personal data.

This construction strikes as innovation when considered in the light of the ECHR, which enshrines a right to respect for private life, but does not enshrine an additional right on the protection of personal data (Pérez Luño 2010, p. 623).[243] It also diverges from the framing sustained by Convention 108 and Directive 95/46/EC, which presented the protection of personal data as serving rights and freedoms in general, and in particular the right to privacy (understood as a right enshrined in Article 8 of the ECHR), but not as related to a sui generis, specific right (Cartabia 2007, p. 33; Vitorino 2003, p. 117).

Although some European countries had already recognised a right to the protection of personal data per se, it is the first time that a supranational level instrument establishes as separate a right to respect for private life, and a right to the protection of personal data (Coudray 2010, p. 314). The coexistence of Articles 7 and 8 of the Charter might be explained in terms of a compromise between divergent national constitutional approaches (those envisioning privacy as encompassing personal data protection v those conceiving of personal data protection as an autonomous fundamental right) (Martínez Martínez 2004, p. 219). But it can also be described, from an EU perspective, as the outcome of an unresolved friction between an established approach and a novel one (Coudray 2010, p. 290).

The Convention had manifestly not respected the prohibition to innovate (Braibant 2001, p. 47; Pati 2012, p. 45). In the way it dealt with the protection of personal data, the Convention apparently attempted to combine the creation of a new right on the protection of personal data, in Article 8 of the Charter, with the restatement of a right that had been construed as being served by the protection of personal data, in Article 7. In a sense, this coexistence contributed to reduce the impact of the change, and to allow for innovation without rupture. But it also raised many questions.

By advancing the right to respect for private life and the protection of personal data as different rights, the Charter puts forward that a distinction can be drawn up

[242] This choice has been described as illustrating a 'laic' tendency to detach private life from the notion of dignity: (Battista Petti 2006, p. 245).

[243] Comparing the Charter to the ECHR and its additional protocols, some have found seven new rights: the dignity of the human person, the integrity of the human person, freedom of research, the right to asylum, the protection of aliens, the protection of children, and the protection of personal data (Loncle 2002, p. 45). See also: (Ehlers 2007b, p. 382). Arguing that innovations were limited: (Amato and Ziller 2007, p. 20). See also: (Brosig 2006, p. 20).

among them (Kranenborg 2008, p. 1090), but it does not clarify the nature of the distinction, or the relations between the distinct rights. Some contend that the right of Article 8 of the Charter has to be regarded as complimentary to Article 7 (Büllesbach et al. 2010, p. 2), or as developing Article 7 for the concrete field of personal data processing (European Union Network of Independent Experts in Fundamental Rights 2006, p. 90), while others have stressed that its mere existence in a way it contradicts certain conceptions of the right to respect for private life (Carlos Ruiz 2003, p. 8). In any case, the simultaneous presence of the two rights appears to offer the possibility to address issues related to the processing of information about individuals either through Article 7 of the Charter, or through Article 8 (Martínez Martínez 2004, p. 327).

6.4.2.2 Content of Article 7 of the EU Charter

Article 7 of the EU Charter reads:

> Article 7– Respect for private and family life
> Everyone has the right to respect for his or her private and family life, home and communications.

The provision unquestionably echoes Article 8 of the ECHR, which sets out:

> Article 8– Right to respect for private and family life
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

There are two main differences between the two articles. First, the Charter's Article 7 refers to a right to respect for 'communications', whereas Article 8 of the ECHR refers to 'correspondence'. This change was intended to mirror the expansion of the notion in the case law of the ECtHR,[244] in the context of the Strasbourg Court's will to keep the reading of the ECHR in line with the needs of contemporary society (Chalmers et al. 2006, p. 255).

Second, the Charter's Article 7 lacks a paragraph equivalent to Article 8(2) of the ECHR, which describes the requirements applicable to interferences with the rights of Article 8(1) of the ECHR to be regarded as lawful. This is due to a deliberate choice made by the Convention drafting the Charter. The Convention wished to replace this kind of clauses, which typically accompany the enshrinement of some ECHR rights, with a limited set of final clauses applying to all the Charter rights, apparently with the purpose of keeping the Charter as short as possible (Calliess 2007, p. 524).

[244] See, for instance: *Klass and others v Germany* [1978] Series A no 28, App. No 5029/71.

As a consequence, Article 7 of the Charter needs to be read in conjunction with the Charter's Article 52, on the 'Scope of guaranteed rights', and in particular with its first paragraph, which establishes:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

This provision is relatively similar to Article 8(2) of the ECHR, but not identical. The words of Article 52(1) recall to some degree the content of the ECHR, but it is uncertain whether those words can be read as having the same meaning of those of Article 8(2) of the ECHR, in particular as interpreted by the Strasbourg Court. For instance, there exists extensive ECtHR case law on the substantive content of the requirement of 'in accordance with the law', an expression that might not be fully equivalent to the reference in Article 52(1) to 'provided for by law'. It is also uncertain whether the principle of proportionality, as applicable in EU law, and to which the EU Charter refers, is comparable to proportionality requirements derived from the condition of being 'necessary in a democratic society' of Article 8(2) of the ECHR, as interpreted by the ECtHR.[245] Additionally, instead of merely mirroring the legitimate purposes set out in Article 8(2) of the ECHR, Article 52(1) of the Charter refers to the notion of 'objectives of general interest recognised by the Union'. These objectives might include purposes that are not identified by Article 8(2) of the ECR as legitimate grounds justifying interferences with the right to respect for private life. As an extra requirement, not foreseen in the ECHR, the Charter establishes that for what it calls 'limitations' (instead of interferences) to be lawful, these limitations need to respect the essential content of the rights affected.

Article 52 of the EU Charter comprises another paragraph relevant for the interpretation of Article 7, namely its third paragraph, which reads as follows:

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

As Article 7 of the Charter undoubtedly mirrors Article 8 ECHR, it follows that, despite any apparent differences between both provisions, the former needs to be read as meaning the same as the latter—at least insofar as they correspond to each other. It becomes thus crucial to determine to what extent do they correspond to each other. In this context, it is possible to argue that the recognition of the protection of personal data as a separate right in the Charter might imply that, at least insofar as this matter is concerned, they might not correspond to each other (Le Bot 2003, p. 806). Similarly, it can also be possible to argue that the content of the right of the Charter's Article 7 might have been affected by the fact that the Charter

[245] See, on the principle of proportionality and EU law: (De Búrca 1993).

devotes a specific Article[246] to environmental protection, taking into account that the ECtHR had addressed environmental issues through the lens of Article 8 of the ECHR, and not outside of it (EU Network of Independent Experts on Fundamental Rights 2003, p. 77).

The final version of the Explanations accompanying the Charter, as elaborated by the Secretariat of the Convention[247] under the authority of the Praesidium in 2000,[248] asserts that the rights guaranteed in Article 7 of the Charter 'correspond' to those ensured by Article 8 of the ECHR. The Explanations also maintain that, as a consequence, both provisions have the same meaning, and they declare that this entails that the limitations that may be legitimately imposed on the rights of Article 7 of the Charter are equivalent to the interferences described by Article 8(2) of the ECHR.[249]

The 2000 Charter and its Explanations were adopted in eleven languages. As the ECHR only has two official language versions, namely English and French, this resulted in the need to translate Article 8 of the ECHR in order to echo its content in Article 7 of the Charter. The different linguistic versions illustrate a general trend to reproduce the structure of the expressions 'private life' and *vie privée*. In Dutch, the text refers to *privé-leven*. In German, to *Privatleben*. In Italian, to *vita privata*. In Portugal and Spanish, to *vida privada*. In Swedish, to *privatliv*. This apparent consistency among languages generates nevertheless some instances of discontinuity with the terminological choices of Directive 95/46/EC. The Directive, for example, referred in its Dutch version not to *privé-leven* but to *persoonlijke levenssfeer*; in its German version not to the *Privatleben*, but the *Privatsphäre*, or, in Spanish, to *intimidad* instead of *vida privada.*

6.4.2.3 Content of Article 8 of the EU Charter

Article 8 of the EU Charter, titled 'Protection of personal data', establishes:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[246] Article 37 of the EU Charter.

[247] The Secretariat was ensured by the General Secretariat of the Council, headed by Jean-Paul Jacqué, of the Council Legal Service (Piris 2010, p. 148).

[248] *Note from the Praesidium: Subject: Draft Charter of Fundamental Rights of the European Union—Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4487/00 CONVENT 50*, CHARTE 4473/00 CONVENT 49 (OR. fr) Brussels, 11.10.2000.

[249] Ibid. 10.

To this Article is also applicable the horizontal clause of Article 52(1) of the Charter, describing possible lawful limitations with the right it establishes. In principle, Article 8 of the Charter is not concerned by Article 52(3), applicable to Charter rights corresponding to ECHR rights, as it cannot be maintained that there is in the ECHR a right corresponding to this right to personal data protection as something exterior to the right to respect for private life, which is already mirrored in Article 7 of the Charter.

The Explanations accompanying the Charter, as prepared in 2000, contend that the Charter's Article 8 is 'based on' both Article 8 of the ECHR and Article 286 of the EC Treaty (as well as on Directive 95/46/EC, and on Convention 108). They are somehow ambivalent on the implications on these linkages. The Explanations suggest that the right to personal data protection is to be exercised under the conditions laid down in Directive 95/46/EC, and that it might be limited under the conditions set out by Article 52 of the Charter,[250] which actually includes various relevant paragraphs: the already mentioned Article 52(1) setting out general requirements for lawful limitations of rights, and Article 52(3), applicable to Charter rights corresponding to ECHR rights, but also Article 52(2), which sets out that Charter rights 'based on' the Treaties shall be exercised under the conditions and within the limits defined by the Treaties.

Of all the possibly relevant sources used for the identification of the rights listed in the Charter, as detailed by its preamble (constitutional traditions and international obligations common to the Member States, the Treaties, the ECHR, and the case law of the ECJ and of the ECtHR), the only ones that are not mentioned are the case law of the ECJ and the ECtHR, and the common constitutional traditions of Member States (Bernsdorff 2003, p. 157).

The structure of Article 8 of the Charter has led some to assert that, contrary to other Articles establishing rights in the Charter, it includes clauses describing possible interferences with the very right it enshrines.[251] From this perspective, the first paragraph of Article 8 would establish a right (to the protection of personal data), whereas the second and the third paragraphs would detail the requirements applicable to the limitations of the right. This would imply that personal data can be processed, but only if 'fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law',[252] ensuring that '(e)veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified', [253] and that compliance with these rules is subject to control by an independent authority.[254]

Conversely, the Charter's Article 8 can also be apprehended as simply following the general structure of the Charter, and, just as Article 7 of the Charter, not dealing with the description of lawful limitations, which are addressed by the Charter's

[250] Ibid. 11.

[251] See, notably: (Siemen 2006, p. 283).

[252] Article 8(2) of Charter.

[253] Ibid.

[254] Ibid. Article 8(3).

Article 52. From this point of view, the three paragraphs of Article 8 of the Charter would jointly describe the right to the protection of personal data, formally granted to everybody in Article 8(1), described in Article 8(2) as requiring that personal data are processed 'fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law',[255] and that '(e)veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified', and encompassing pursuant to Article 8(3) the existence of an independent supervisory authority.

These two possible readings of Article 8 of the Charter identity as its basic elements, be it conceived of as conditions for limiting the right, or envisaged as requirements for its substantiation, the following six constituents:[256]

- the requirement of fair processing;
- the requirement of processing for specified purposes;
- the requirement of legitimate basis, which can be a basis laid down by law, or the consent of the person concerned;
- a right of access to data;
- a right to have data rectified; and
- independent supervision.

All these elements have precedents in international instruments on the protection of personal data. They can crucially be found in Directive 95/46/EC,[257] which emerges thus as a major source of inspiration (Flauss 2002, p. 69). Many of them can also be traced back to Convention 108,[258] but nevertheless they were incorporated in Article 8 of the EU through the prism of Directive 95/46/EC (Flauss 2002, p. 68), which implies, notably, that they are applicable to personal data in general, and not only to the automated processing of personal data. The only element that is alien to data protection as configured in the context of the Council of Europe is the allusion to the requirement of legitimate basis, incorporating an explicit mention of consent as possible legitimate basis. The linkage of this notion of consent, whose place in Article 8 of the Charter has been criticised (Rouvroy and Poullet 2009), can be traced back, trough Directive 95/46/EC, to the first German federal data protection Act, of 1977.[259]

[255] Ibid. Article 8(2).

[256] Referring instead to four principles, concretely: a scope of application covering all personal data (and thus differing from the sole application to 'sensitive' data), subjective rights, certain limitations imposed on those processing data, and the existence of a data protection authority: (Poullet 2006, p. 216; Büllesbach et al. 2010, p. 3). Se also, referring to three principles: (Poullet 2010).

[257] Fair processing in Article 6(1)(a) of Directive 95/46/EC; purpose specification in Article 6(1)(b); legitimate basis in Article 7; right of access in Article 12(a); right of rectification in Article 12(b), independent supervision in Article 28.

[258] Fair processing in Article 5(a) of Convention 108; purpose specification in its Article 5(b); right of access in Article 8(b); right of rectification in Article 8(c). The requirement of supervision by an independent authority was integrated in 2001 into the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No.: 181). Arguing that there are in Article 8 of the Charter elements of all the instruments mentioned in the Explanations: (Rey Martínez 2009, p. 333).

[259] See Chap. 3, Sect. 3.1.3, of this book.

A number of elements which could be considered well-established principles applicable to the processing of personal data are not mentioned in Article 8 of the Charter: for instance, the right to receive information, the idea of control articulated through a right to erasure or cancellation, or security and confidentiality obligations (Carlos Ruiz 2003, p. 39).

Article 8 of the Charter has been described as an innovative fundamental right (Braibant 2001, p. 47) that was, however, not really new (Bernsdorff 2003, p. 160). It is certainly rooted in previously existing instruments. It innovates to the extent that it establishes that the elements mentioned deserve to be protected as elements of a fundamental right deserving protection per se (Docquir 2008, p. 41), and that the protection is not exclusively granted to data in a way or another related to the right to respect for private life, but to personal data in general. In this sense, it goes beyond the scope of the protection granted on the basis of the ECHR, and of the common constitutional traditions of the Member States (Kühling 2011, p. 489).

The right's name echoes the significance of previous instruments on personal data protection, but nevertheless brings forward a new notion: the 'protection of personal data', a phrase that could not be found as such in Directive 95/46/EC,[260] and only incidentally in Convention 108 (which was overtly devoted to 'data protection').[261] The inclusion of the adjective personal in the Article's heading led to the German version not using *Datenschutz* but, instead, *Schutz personenbezogener Daten*. Some language versions designated 'personal data' through specific notions already surfaced in Directive 95/46/EC and in previous international instruments, such as the French *données à caractère personnel* ('data of personal nature') (instead of the also linguistically possible *données personnelles*).[262] The Spanish and Italian version similarly opted for *datos de carácter personal* and *dati di carattere personale*, respectively, even if in the Directive are also used the expressions *datos personales* and *dati personali.* Perhaps one of the most noticeable differences appeared in the Swedish text, which referred to *skydd av personuppgifter* ('protection of personal data') thus relying on an expression different from the word normally used in Swedish to refer to Directive 95/46/EC: *dataskydds* ('data protection').

6.5 Summary

This chapter has inquired into the recognition of EU fundamental rights, and has investigated the coming into being of personal data protection as a fundamental right of the EU. The notion of EU fundamental rights was endorsed by EU law in

[260] Which merely uses once the words 'personal data protection', referring to a 'personal data protection official' (Article 18(2) of Directive 95/46/EC).

[261] There is nonetheless a reference to the 'protection of personal data' in relation to security obligations (Article 7 of Convention 108).

[262] Already present in the OECD Guidelines: *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*.

response to the resistance of some Member States to accept that the EU might deprive them, in certain circumstances, of the possibility to assess the validity of some laws in the light of their national (fundamental) rights.

Initially, EU law recognised as fundamental rights those endorsed by international treaties signed by the Member States, such as the ECHR, and those identified as being common to the national constitutional traditions of the Member States. Eventually, however, EU institutions decided it was necessary to reinforce this system of fundamental rights protection with the elaboration of a specific EU list of rights. This exercise opened the possibility to endorse, in addition to the rights already identified as existent, some rights considered as inexistent but regarded as necessary in the light of contemporary needs. In this context saw the light the EU right to the protection of personal data, established in 2000 by Article 8 of the Charter of Fundamental Rights of the EU. The Explanations accompanying the EU Charter declared that the right to personal data protection was based on a series of instruments and provisions that, as a matter of fact, did not mention any right to personal data protection. Such instruments and provisions actually linked the protection of personal data to the safeguarding of rights and freedoms in general, and to ensuring the right to privacy in particular. Some Member States recognised by 2000 rights similar to the protection of personal data, but they were a minority, and this approach did not, in any case, constitute a common constitutional tradition among them. The EU Charter enshrining a new right to the protection of personal data, adopted against such heterogeneous background, did not acquire legally binding status until 9 years after its solemn proclamation.

References

Alexy, Robert. 2010. *A Theory of Constitutional Rights* (originally published 2002). Oxford: Oxford University Press.

Amato, Giuliano, and Jacques Ziller. 2007. *European Constitution: Cases and Materials in EU and Member State's Law*. Cheltenham: Edward Elgar.

Arenas Ramiro, Mónica. 2006. *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Tirant Lo Blanch.

Arenas Ramiro, Mónica. 2007. El derecho a la protección de datos personales como garantía de las libertades de expresión e información. In *Libertad en Internet: La Red y las libertades de expresión e información*, ed. Lorenzo Cotino Hueso, 355–385. Valencia: Tirant Lo Blanch.

Article 29 Data Protection Working Party. 1999. Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights. WP 26. Brussels.

Article 29 Data Protection Working Party. 2002. Fifth annual report: On the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European union and in third countries covering the year 2000, Part II. WP 54. Brussels.

"Basic Law for the Federal Republic of Germany, Translated by Christian Tomuschat and David P. Currie, Translation Revised by Christian Tomuschat and Donald P. Kommers in Cooperation with the Language Service of the German Bundestag" 2010. Deutscher Bundestag.http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html. Accessed 10 March 2013.

Battista Petti, Giovanni. 2006. *La Costituzione Europea e la tutela civile dei dirtti umani* (Aggiornato alla Legge 15 dicembre 2005, N. 280). Santarcangelo di Romagna: Maggioli Editore.

Bellos, David. 2011. *Is That a Fish in Your Ear? The Amazing Adventure of Translation*. London: Penguin Books.

Bernhardt, Rudolf. 1976. The problems of drawing up a catalogue of fundamental rights for the European communities. *Bulletin of the European Communities*, 76 (Suppl 5): 18–69.

Bernsdorff, Norbert. 2003. Kapitel II, Freiheiten: Artikel 6 Bis 19. In *Kommentar zur Charta der Grundrechte der Europäischen Union*, ed. Jürgen Meyer, 135–262. Baden-Baden: Nomos Verlagsgesellschaft.

Blanchard, David. 2001. *La Constitutionnalisation de l'Union européenne*. Rennes: Éditions Apogée.

Braibant, Guy. 1998. Données personnelles et société de l'information: Rapport au Premier Ministre sur la transposition en Droit français de la Directive No 95/46 (Rapport Braibant).

Braibant, Guy. 2001. *La Charte des Droits fondamentaux de l'Union européenne*. Paris: Editions du Seuil.

Briboisia, Emmanuele, and Sébastien Van Drooghenbroeck. 2009. Emprunts et migrations entre le Droit de l'Union européenne et le Droit du Conseil de l'Europe. In *Traduction et droits européens: Enjeux d'une rencontre : Hommage au Recteur Michel van de Kerchove*, eds. Antoine Bailleux, Yves Cartuyvels, Hugues Dumont, and François Ost, 133–180. Bruxelles: Facultés universitaires Saint-Louis.

Brosig, Malte. 2006. Human rights in Europe: An introduction. In *Human rights in Europe: A Fragmented Regime?* ed. Malte Brosig, 9–29. Frankfurt a. M.: Peter Lang.

Büllesbach, Alfred, Serge Gijrath, Yves Poullet, and Corien Prins, ed. 2010. *Concise European IT Law*. 2nd ed. Alphen aan den Rijn: Kluwer Law International.

Burkert, Herbert. 1999. Privacy/data protection: A German/European perspective. In Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass, 43–69. http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf.

Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. London: Kluwer Law International.

Bygrave, Lee A. 2010. Privacy and data protection in an international perspective. *Scandinavian Studies in Law* 56:165–200.

Calliess, Christian. 2007. The Charter of fundamental rights of the European Union. In *European Fundamental Rights and Freedoms*, ed. Dirk Ehlers, 518–539. Berlin: De Gruyter.

Carlos Ruiz, Miguel. 2003. El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo* 7 (14): 7–43.

Cartabia, Marta. 2007. L'ora dei diritti fondamentali nell'Unione Europea. In *I Diritti in Azione: Universalità e Pluralismo dei Diritti Fondamentali nelle Corti Europee*, ed. Marta Cartabia, 13–66. Bologna: Il Mulino.

Chalmers, Damian, Christos Hadjiemmanuil, Giorgio Monti, and Adam Tomkings. 2006. *European Union Law*. Cambridge: Cambridge University Press.

Comité des Sages chaired by Maria de Lourdes Pintasilgo. 1996. For a Europe of civic and social rights (Brussels, October 1995–February 1996). Office for Official Publications of the EC.

Commission nationale de l'informatique et des libertés (CNIL). 2012. Conférence de Presse 10 Juillet 2012: Présentation du 32ème Rapport d'activité 2011. Paris.

Commission of the European Communities. 1975. Report on European Union. Bulletin of the European Communities Supplement 5/75.

Commission of the European Communities. 1976. Special Report of the Commission of February 4, 1976 to the European Parliament and the Council on 'The Protection of Fundamental Rights as Community Law is Created and Developed' (Protection of Fundamental Rights Within the European Community). Bulletin of the European Communities Supplement 5/76.

Coudray, Ludovic. 2010. *La protection des données personnelles dans l'Union européenne : Naissance et consécration d'un droit fondamental*. Berlin: Éditions universitaires européennes.

Craig, Paul, and Gráinne De Búrca. 2011. *EU Law: Text, Cases and Materials* (5th ed.). Oxford: Oxford University Press.

Cremer, Hans-Joachim. 2011. *Human Rights and the Protection of Privacy in Tort Law: A Comparison between English and German Law*. London: Routledge.

De Búrca, Gráinne. 1993. The principle of proportionality and its application in EC law. *Yearbook of European Law* 13 (1): 105–150.

De Búrca, Gráinne. 2011. The evolution of EU Human Rights Law. In *The Evolution of EU law* (2nd ed.), eds. Paul Craig and Gráinne De Búrca, 465–497. Oxford: Oxford University Press.

De Domingo, Tomás. 2011. La Teoría de la Justicia del Neoconstitucionalismo: Los derechos fundamentales como núcleo del bien común. In *Los Derechos Fundamentales en el Sistema Constitucional: Teoría General e Implicaciones Prácticas*, eds. Antonio Luis Martínez-Pujalte and Tomás De Domingo, 5–29. Granada: Editorial Comares.

De Domingo, Tomás, and Antonio Luis Martínez-Pujalte. 2011. La interpretación de la garantía del contenido esencial y la estructura de los derechos fundamentales. In *Los Derechos Fundamentales en el Sistema Constitucional: Teoría General e Implicaciones Prácticas*, eds. Antonio Luis Martínez-Pujalte and Tomás De Domingo, 31–55. Granada: Editorial Comares.

De Schutter, Olivier. 2010. *International Human Rights Law*. Cambridge: Cambridge University Press.

De Witte, Bruno. 1999. The past and future role of the European Court of Justice in the protection of human rights. In *The EU and Human Rights*, eds. Philip Alston, Mara Bustelo, and James Heenan, 859–897. Oxford: Oxford University Press.

Desgens-Pasanau, Guillaume. 2012. *La protection des données à caractère personnel: La Loi "Informatique et Libertés "*. Paris: LexisNexis.

Dias Venâncio, Pedro. 2007. A previsão constitucional da utilização da informática. *Revista de Estudos Politécnicos* 8:243–264.

Docquir, Benjamin. 2008. *Le droit à la vie privée*. Bruxelles: De Boeck, Larcier.

Douglas-Scott, Sionaidh. 2006. A tale of two Courts: Luxembourg, Strasbourg and the growing European human rights acquis. *Common Market Law Review* 43:629–665.

Dreyer, Emmanuel. 2006. Du caractère fondamental de certains droits. *Droit Prospectif: Revue de la Recherche Juridique* 31 (113): 551–580.

Dutheil de la Rochère, Jacqueline. 2003. La place de la Charte des Droits fondamentaux de l'Union européenne dans la Constitution européenne. In *Constitution européenne, démocratie et Droits de l'homme*, eds. Gérard Cohen-Jonathan and Jacqueline Dutheil de la Rochère, 229–239. Bruxelles: Bruylant.

Ehlers, Dirk. 2007a. The fundamental freedoms of the European communities. In *European fundamental Rights and Freedoms: General Principles,* ed. Dirk Ehlers, 175–225. Berlin: De Gruyter.

Ehlers, Dirk. 2007b. The fundamental rights of the European Union: General principles. In *Fundamental Rights and Freedoms: General Principles*, ed. Dirk Ehlers, 371–398. Berlin: De Gruyter.

Electronic Privacy Information Center (EPIC), and Privacy International (PI). 2007. Privacy & Human Rights 2006: An international survey of privacy laws and developments. Washington, D.C. and London: EPIC / PI.

EU Network of Independent Experts on Fundamental Rights. 2003. Report on the situation of fundamental rights in the European union and its member states in 2002.

European Commission. 1995. Note on seminar on 'Openness and Transparency in the European Union' on 22 November 1995, NR(95). Brussels.

European Union Network of Independent Experts in Fundamental Rights. 2006. Commentary of the Charter of fundamental rights of the European Union.

Expert Group on Fundamental Rights. 1999. *Affirming Fundamental Rights in the European Union: Time to Act*. Brussels: European Commission.

Flauss, Jean-François. 2002. Les libertés fondamentales traditionnelles: Nouvelles approches et solutions originales? In *The Charter of Fundamental Rights and Constitutional Development in the EU*, ed. Wolfgang Heusel, 63–81. Köln: Bundesanzeiger.

García Roca, Javier, and Pablo Antonio Fernández Sánchez. 2009. Prefacio. In *Integración europea a través de derechos fundamentales: De un sistema binario a otro integrado*, eds. Javier García Roca and Pablo Fernández Sánchez, xix–xxxii. Madrid: Centros de Estudios Políticos y Constitucionales.

Gómez Navajas, Justa. 2005. *La protección de los datos personales*. Cizur Menor: Aranzadi.
Grewe, Constance, and Hélène Ruiz Fabri. 1995. *Droits constitutionnels européens*. Paris: Presses Universitaires de France.
Guerrero Picó, María del Carmen. 2006. *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Cizur Menor: Thomson Civitas.
Guild, Elspeth, and Guillaume Lesieur. 1998. *The European Court of Justice on the European Convention on Human Rights: Who Said What, When?* London: Kluwer Law International.
Harpaz, Guy. 2009. The European Court of Justice and its relations with the European Court of Human Rights: The quest for enhanced reliance, coherence and legitimacy. *Common Market Law Review* 46:105–141.
Hornung, Gerrit, and Christoph Schnabel. 2009. Data potection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Report* 25:84–88.
Horspool, Margot. 2006. Over the rainbow: Languages and Law in the future of the European Union. *Futures* 38 (2): 158–168.
Jacqué, Jean-Paul. 1980. La Convention pour la Protection des Personnes à l'égard du Traitement Automatisé des Données à Caractère Personnel. *Annuaire Français de Droit International* 26:773–789.
Kommers, Donald P. 1997. *The Constitutional Jurisprudence of the Federal Republic of Germany*. London: Duke University Press.
Koops, Bert-Jaap, Ronald Leenes, and Paul De Hert. 2007. Constitutional rights and new technologies: A comparative study covering Belgium, Canada, France, Germany, Sweden, and the United States. Tilburg: Tilburg Institute for Law, Technology, and Society (TILT).
Korff, Douwe. 2002. European Commission study on implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49): Comparative summary of national laws. European Commission.
Korff, Douwe. 2010. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Working Paper no. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments. European Commission.
Kranenborg, Herke. 2008. Access to documents and data protection in the European Union: On the public nature of personal data. *Common Market Law Review* 45 (4): 1079–1114.
Kühling, Jürgen. 2011. Multilevel Constitutional jurisdiction. In *Principles of European constitutional Law* (Revised 2nd ed.), eds. Armin Von Bogdandy and Jürgen Bast, 479–514. Oxford: Hart Publishing.
Lawson, Rick. 1994. Confusion and conflict? Diverging interpretations of the European Convention on Human Rights in Strasbourg and Luxembourg. In *The Dynamics of the Protection of Human Rights in Europe: Essays in honour of Henry G Schermers*, eds. Rick Lawson and Matthijs De Blois, 219–252. The Hague: Nijhoff.
Le Bot, Olivier. 2003. Charte de l'Union européenne et Convention de Sauvegarde des Droits de l'homme: La coexistence de deux catalogues de Droits fondamentaux. *Revue trimestrielle de Droit européen* 55:781–811.
Loncle, François. 2002. La Charte des Droits fondamentaux : Le référentiel des valeurs de l'Europe. In *La Charte des Droits fondamentaux et le développement constitutionnel de l'Union européenne*, ed. Wolfgang Heusel, 43–50. Köln: Bundesanzeiger.
Lugaresi, Nicola, and Silvia Bertazzo. 2009. La tutela del diritto alla privacy davanti al Garante per la Protezione dei Dati Personali: Profili sostanziali e procedurali. In *La Politica della Privacy: Tra Tutela dei Diritti e Garanzia dei Sistemi*, ed. Bruno Dente, Nicola Lugaresi, and Maria Stella Righettini, 23–140. Firenze: Passigli.
Martín y Pérez de Nanclares, José. 2008. Comentario Al Artículo 8 Sobre Protección de Datos de Carácter personal. In *Carta de los Derechos Fundamentales de la Unión Europea: Comentario Artículo Por Artículo*, ed. Luis N. González Alonso, 224–243. Madrid: Fundación BBVA.
Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.

Mischo, Jean. 2003. Hoechst, Colas, Roquette: Illustration d'une convergence. In *Une communauté de droit: Festchrift für Gil Carlos Rodríguez Iglesias*, eds. Ninon Colneric, David Edward, Jean-Pierre Puissochet, and Dámaso Ruiz-Jarabo Colomer, 137–145. Berlin: Berliner Wissenschafts-Verlag.

Moderne, Franck. 2000. La notion de droit fondamental dans les traditions constitutionnelles des États membres de l'Union européenne. In *Réalité et perspectives du droit Communautaire des droits fondamentaux*, eds. Frédéric Sudre and Henri Labayle. Bruxelles: Bruylant.

Morange, Jean. 2003. Liberté. In *Dictionnaire de la culture juridique*, eds. Denis Alland and Stéphane Rials, 950. Paris: Quadrige/Lamy-PUF.

Morijn, John. 2006. Balancing fundamental rights and common market freedoms in Union law: Schmidberger and Omega in the light of the European constitution. *European Law Journal* 12 (1): 15–40.

Murillo de la Cueva, Pablo Lucas. 1999. La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos* 104 (abril-junio): 35–60.

Murillo de la Cueva, Pablo Lucas. 2009. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. In *El derecho a la autodeterminación informativa*, eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 11–80. Madrid: Fundación Coloquio Jurídico Europeo.

Öberg, Ulf. 1998. Public access to documents after the entry into force of the Amsterdam Treaty: Much Ado About Nothing? European Integration Online Papers (EIoP) 2. http://eiop.or.at/eiop/texte/1998-008a.htm.

Oliver, Peter. 2009. The protection of privacy in the economic sphere before the European Court of Justice. *Common Market Law Review* 46:1443–1483.

Ordóñez Solís, David. 2011. *Privacidad y protección judicial de los datos personales*. Barcelona: Bosch.

Oreja Aguirre, Marcelino, and Francisco Fonseca Morillo. 1998. *El Tratado de Ámsterdam: Análisis y comentarios, Volumen I*. Madrid: McGraw Hill.

Orti Vallejo, Antonio. 1994. El nuevo derecho fundamental (y de la personalidad) a la libertad informática: A propósito de la STC 254/1993, de 20 de julio. *Derecho Privado y Constitución* 2 (enero-abril): 305–332.

Pati, Roza. 2012. Rights and their limits: The constitution for Europe in international and comparative legal perspective. *Berkeley Journal of International Law* 23:223.

Pérez Luño, Antonio Enrique. 2010. *Derechos Humanos, Estado de Derecho y Constitución* (10th ed.). Madrid: Tecnos.

Pernice, Ingolf, and Ralf Kanitz. 2004. Fundamental Rights and Multilevel Constitutionalism in Europe. WHI Paper 7/04. Berlin: WHI Paper 7/04 (Walter Hallstein-Institut für Europäisches Vergassungsrecht), Humboldt-Universität zu Berlin.

Picod, Fabrice. 2000. Les sources. In *Réalité et perspectives du droit communautaire des droits fondamentaux*, eds. Frédéric Sudre and Henri Labayle, 125–185. Bruxelles: Bruylant.

Piñar Mañas, José Luis. 2009. Protección de datos: Origen, situación actual y retos de futuro. In *El derecho a la autodeterminación informativa*, eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 81–179. Madrid: Fundación Coloquio Jurídico Europeo.

Piris, Jean-Claude. 2010. *The Lisbon Treaty: A Legal and Political Analysis*. Cambridge: Cambridge University Press.

Poiares Maduro, Miguel. 1999. Striking the elusive balance between economic freedom and social rights in the EU. In *The EU and Human Rights*, eds. Philip Alston, Mara Bustelo, and James Heenan, 449–472. Oxford: Oxford University Press.

Pospíšil, Filip, and Marek Tichy. 2010. Comparative Study on Different Approaches to New Privacy Challenges, In *Particular in the Light to Technological Developments: Country Study A.1*. Czech Republic: European Commission.

Poullet, Yves. 2006. The Directive 95/46/EC: Ten years after. *Computer Law & Security Report* 22:206–217.

Poullet, Yves. 2010. About the E-privacy Directive: Towards a Third Generation of Data Protection Legislation? In *Data Protection in a Profiled World*, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert, 3–30. Dordrecht: Springer.

Prakke, Lucas, and Constantin Kortmann. 2004. *Constitutional Law of 15 Member States*. Deventer: Kluwer Legal Publishers.

Rey Martínez, Fernando. 2009. ¿Cómo nacen los derechos? Posibilidades y límites de la creación judicial de derechos. In *Integración europea a través de derechos fundamentales: De un sistema binario a otro integrado*, eds. Javier García Roca and Pablo Antonio Fernández Sánchez, 327–352. Madrid: Centros de Estudios Políticos y Constitucionales.

Rigaux, François. 1990. *La protection de la vie privée et des autres biens de la personnalité*. Bruxelles: Bruylant.

Rincón Eizaga, Lorena. 2008. Human rights in the European Union: Conflict between the Luxembourg and Strasbourg Courts regarding interpretation of Article 8 of the European Convention on human rights. *Revista Colombiana de Derecho Internacional* 11 (mayo): 119–154.

Rivers, Julian. 2010. A theory of constitutional rights and the British constitution. In *A Theory of Constitutional Rights*, ed. Robert Alexy, xvii–l. USA: Oxford University Press.

Rodotà, Stefano. 2009. *La vita e le regole: Tra diritto e non diritto*. Milano: Feltrinelli.

Rodotà, Stefano. 2010. Nouvelles technologies et droits de l'homme: Faits, interprétations, perspectives. *Mouvements* 62 (avril-juin): 56–70.

Rouvroy, Antoinette, and Yves Poullet. 2009. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In *Reinventing Data Protection?*, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 45–76. Dordrecht: Springer.

Saarenpää, Ahti. 1997. Data protection: In pursuit of information: Some background to, and implementations of, data protection in Finland. *International Review of Law Computers & Technology* 11 (1): 47–64.

Sáenz de Santamaría, Paz Andrés. 2008. La Carta de los Derechos Fundamentales de la Unión Europea en la práctica española. *Revista de Derecho de la Unión Europea* 15:233–255 (2° semestre).

Safjan, Marek. 2001. The right to privacy and personal data protection in the information society. In Council of Europe, Proceedings of the European Conference on Data Protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and Future, 19 November, Warsaw.

Schneider, Peter. 1979. Peculiaridad y función de los derechos fundamentales en el Estado Constitucional Democrático. *Revista de Estudios Políticos* 7:7–36.

Siemen, Birte. 2006. *Datenschutz als Europäisches Grundrecht*. Berlin: Duncker & Humblot.

Silveira, Luis. 2007. Private life—A sensitive data in Portugal. *Dataprotectionreview.eu:* edited by the Data Protection Agency of Madrid, 2.

Smog. 1999. Cold blooded old times. *Knock Knock.* Domino.

Solanes Corella, Ángeles, and María Belén Cardona. 2005. *Protección de datos personales y derechos de los extranjeros inmigrantes*. Valencia: Tirant Lo Blanch.

Spielmann, Dean. 1999. Human rights case law in the Strasbourg and Luxembourg Courts: Conflicts, inconsistencies, and complementarities. In *The EU and Human Rights*, eds. Philip Alston, Mara Bustelo, and James Heenan, 757–780. Oxford: Oxford University Press.

Spinelli, Altiero. 1992. *Diario Europeo: 1976–1986*. Bologna: Il Mulino.

Steele, Jonathan. 2002. Data protection: An opening door? The relationship between accessibility and privacy in Sweden in an EU perspective. *Liverpool Law Review* 24:19–39.

Sudre, Frédéric. 2005. *Droit européen et international des droits de l'homme* (7th ed.). Paris: Presses Universitaires de France.

Swedish Ministry of Justice. 1996a. *Swedish position concerning openness in the European institutions*. Stockholm.

Swedish Ministry of Justice. 1996b. *Swedish working document concerning access to documents in the European institutions*. Stockholm.

Székely, Iván. 2008. Hungary. In *Global Privacy Protection: The First Generation*, eds. James B. Rule and Graham Greenleaf, 174–206. Cheltenham: Edward Elgar Publishing.

Tiberi, Giulia. 2007. Riservatezza e protezione dei dati personali. In *I diritti in azione: Universalità e pluralismo dei diritti fondamentali nelle Corti europee*, ed. Marta Cartabia, 349–387. Bologna: Il Mulino.

Vitorino, Antonio. 2003. La Cour de Justice et les droits fondamentaux depuis la proclamation de la Charte. In *Une communauté de droit: Festchrift für Gil Carlos Rodríguez Iglesias*, eds. Ninon Colneric, David Edward, Jean-Pierre Puissochet, and Dámaso Ruiz-Jarabo Colomer, 111–126. Berlin: Berliner Wissenschafts-Verlag.

Walter, Christian. 2007. The notion of European fundamental rights and freedoms. In *European Fundamental Rights and Freedoms*, ed. Dirk Ehlers, 1–24. Berlin: De Gruyter.

Wetzel, Joseph R. 2003. Improving fundamental rights protection in the European Union: Resolving the conflict and confusion between the Luxembourg and Strasbourg courts. *Fordham Law Review* 71:2823–2862.

Chapter 7
The Right to the Protection of Personal Data and EU Law

Privacy is a nothingness these days.

(Gaeoudjiparl 2012)

The Charter of Fundamental Rights of the European Union (EU) was supposed to contribute to clarity, rendering more apparent, and more accessible to EU citizens, the rights and principles regarded by the EU as 'fundamental'. However, it only acquired legally binding force nine years after the European Parliament, the Council and the European Commission solemnly proclaimed it. And when the Lisbon Treaty finally granted to it legally binding status, the Charter merely became one source of EU fundamental rights among multiple other sources—others that, contrary to the Charter, did not recognise any EU right to the protection of personal data as such.

This chapter explores the coming into being of the EU right to personal data protection in this particular context. It is divided into two parts: the first reviews the situation until the entry into force of the Lisbon Treaty in December 2009, while the second investigates the post-Lisbon state-of-affairs.

7.1 A Transition: 2000–2009

If some had envisioned the Charter's proclamation as a step towards legal certainty, in practice the new instrument did not immediately reinforce any certainty at all. Before 2000, the European Court of Justice (ECJ) had been granting recognition to a series of rights that corresponded almost perfectly to those of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), even if taking also into account the constitutional traditions common to the Member States. With the Charter's proclamation, the EU moved from such roughly unitary system of identification of applicable fundamental rights to a structurally binary one. This shift represented in itself a factor of legal uncertainty (Le Bot 2003, p. 787).

A number of important issues soon appeared as problematically unsettled. First, the ECHR and the Charter, despite their many resemblances, do not comprise identical provisions on applicable rights, or on the right's permissible limitations, opening up the question of how to deal with possible discrepancies. A second factor of

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_7,

legal uncertainty was linked to the peculiar status of the Charter, which had been solemnly proclaimed by EU institutions, but was not binding as such. And an additional factor of uncertainty surfaced specifically in those cases where the Charter had arguably subtly advanced new rights. The Charter, sometimes described as an innovative instrument allowing the EU 'to keep abreast of changes in society and scientific and technological developments' (European Commission 2010b, p. 3), was also simultaneously supposedly merely reaffirming existing rights.[1] The question arose thus, in relation to seemingly unprecedented rights such as the right to the protection of personal data, of whether the Charter was merely reaffirming with its provisions previously existing rights, reaffirming and updating them, or actually increasing their number, and of to what extent it was doing each of these things. All in all, it was in any case difficult to argue that the Charter had rendered EU fundamental rights more 'predictable' (European Commission 2010b, p. 3).

7.1.1 The Moving Conceptualisation of Personal Data Protection

After the proclamation of the EU Charter, and on the basis of its Article 8, the literature started to increasingly acknowledge the existence of a notion of (personal) data protection as autonomous—at least partially. Before 2000, it was relatively common to assert that the right to respect for private life included the protection of personal data, the former being a notion wider than the latter. The protection of personal data was often regarded as the 'informational dimension' of the right to respect for privacy (Benyekhlef 1996, p. 91), and thus a mere facet of a broader notion that included many others.

This approach became progressively less predominant, and gradually gave place to the idea that in fact there existed two separate, distinct notions: on the one hand, privacy or the respect for private life, and, on the other, the protection of personal data, also often simply referred to as 'data protection'. Prototypically, the co-existence of these two notions was put forward together with the assertion that privacy and (personal) data protection were nevertheless 'closely related' (Bougettaya 2006, p. 41; Kranenborg 2008, p. 1090).[2] And, in some cases, this tight relationship between privacy and (personal) data protection was described in terms of a partial overlap.

The image of the partial overlap allowed to synthesise the more traditional approach of envisaging (personal) data protection as integral to privacy/respect for private life (or, in other terms: *privacy > data protection*), and the more modern conception of (personal) data protection as different from privacy/respect for private life (*privacy # data protection)*. The representation of a partial overlap supported both theories as compatible: yes, in a way the protection of personal data was part of a wider right to respect for private life, or right to privacy, but at the same time

[1] See preamble to the EU Charter.

[2] Describing them as 'closely linked': (Bygrave 2010, p. 168).

it was also different from the right to respect for private life, or right to privacy (Hustinx 2005, p. 62).[3] The right to personal data protection could thus be described as resulting from a widening of the right to privacy, but autonomous (Rodotà 2009, p. 79).

In spite of the initial unsettled legal status of the Charter, of the many uncertainties of its place in the EU's fundamental rights architecture, and of the status of the right to the protection of personal data, Article 8 of the Charter soon started to be integrated in EU secondary law.

7.1.2 Data Protection and Privacy in EU Secondary Law

In the 1990s EU law had embraced the approach of Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), according to which 'data protection' serves the insurance of all rights and freedoms, but notably of the right to privacy. In the 2000s, this formula lived on, but it started to be increasingly accompanied by innovative joint occurrences of the notions of data protection and privacy,[4] often mentioned together in phrases characterised by their ambiguity (Korff 2004, p. 6). Early references to the Charter's Article 8 tended to pop up in EU law always in conjunction with references to Article 7 of the Charter, on the right to respect for private life. But, despite the repeated binding of the notions, the exact nature of the relation between them was left undetermined.

An early example of an ambivalent juxtaposition of the notions of privacy and data protection in post-2000 EU law can be found in Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society,[5] of 2001. The preamble to Directive 2001/29/EC asserts that some rights-management information systems may, depending on their design, 'process personal data about the consumption patterns of protected subject-matter by individuals

[3] An example in a policy document: (Article 29 Data Protection Working Party 2007, p. 7). Arguing that the protection of personal data can only be partially accommodated under the right to respect for private life: (Terrasi 2008, p. 392). Stating that data protection is 'at least partly subsumed within the right to privacy in Article 8 ECHR': (Oliver 2009, p. 1455). Portraying data protection as 'both broader and more specific than the right to privacy': (Gutwirth and Hildebrandt 2010, p. 37). An account of privacy and data protection in terms of opacity tools v transparency tools (based on their roles in the democratic constitutional state) similarly argued that privacy and data protection 'pre-suppose each other and are intertwined': (Gutwirth 2007, p. 63).

[4] As a counter-example, there are references to Directive 95/46/EC, and to personal data, in a Directive lacking any allusion to privacy: Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16). The provision of Directive 2004/48/EC that mentions 'personal data', however, does not specifically refer to the protection of personal data, but rather to 'the protection of confidentiality of information sources or the processing of personal data' (Article 8(3)(e) of Directive 2004/48/EC).

[5] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

and allow for tracing of on-line behaviour', detailing that such technical means 'should incorporate *privacy*[6] safeguards in accordance with Directive 95/46/EC'.[7] This might be read as implying that Directive 95/46/EC is about 'privacy' and about 'privacy safeguards'. Another provision of Directive 2001/29/EC, however, states that the instrument shall be implemented without prejudice to provisions concerning 'data protection and privacy'.[8] Which are exactly these alluded 'data protection and privacy' provisions? Are they something different than those on just privacy (supposedly embodied by Directive 95/46/EC)? It is very much unclear.

7.1.2.1 Directive 2002/58/EC

Personal data protection and privacy had already been prominently mentioned together in Directive 97/66/EC,[9] on the processing of personal data and the protection of privacy in the telecommunications sector. In 2002, that Directive was replaced with Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector.[10]

As recalled in the preamble to Directive 2002/58/EC, Directive 97/66/EC had 'translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector'.[11] Just like Directive 97/66/EC, Directive 2002/58/EC was however not exclusively concerned with particularising the provisions of Directive 95/46/EC for a specific sector (Rosier 2008, p. 353): it also aimed to complement those provisions,[12] notably by providing protection for the confidentiality of communications,[13] envisioned, at least in the English version of Directive 2002/58/EC, as an element of the notion of 'privacy'.

Directive 2002/58/EC has an official heading, like all EU directives. But it also has an official short name, placed between parentheses after the official heading. In the English version, the short name is 'Directive on privacy and electron-

---

[6] Emphasis added.

[7] Recital 57. French version: *'incorporer les principes de protection de la vie privée';* German: *'dem Schutz der Privatsphäre';* Dutch: '*de persoonlijke levenssfeer';* Spanish: '*respeto de la intimidad*'; Italian: '*salvaguardia della vita privata*'.

[8] Article 9 of Directive 2001/29/EC. French version: '*la protection des données personnelles et le respect de la vie privée*'; German version: '*Datenschutz und Schutz der Privatsphäre*'; Dutch: '*gegevensbescherming en persoonlijke levenssfeer*'; Spanish: '*la protección de datos y el derecho a la intimidad*'; Italian: '*la tutela dei dati e il rispetto della vita privata*'.

[9] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1997] OJ L24/1. See Chap. 5, Sect. 5.2.2 of this book.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

[11] Recital 4 of Directive 2002/58/EC.

[12] Article 2(1) of Directive 2002/58/EC.

[13] Ibid. Recital 3.

ic communications', which stresses the instrument's relation with 'privacy', also mentioned in the Directive's official heading.[14] In German, however, the official short name of Directive 2002/58/EC is *'Datenschutzrichtlinie für elektronische Kommunikation'* (or 'Directive on data protection for electronic communications'), which highlights its relationship not with privacy but with data protection, and contrasts with the reference to the *Schutz der Privatsphäre* ('protection of the private sphere') alluded to in the German heading. The Dutch version uses for the Directive's short name the word *privacy*, appearing here as a Dutch word ('*richtlijn betreffende* privacy[15] *en elektronische communicatie')*, even if the Directive's heading mentions *de bescherming van de persoonlijke levenssfeer*. Similarly, the Spanish version refers to the protection of *intimidad* in the heading, but to *privacidad* in its short name.

According to its preamble, Directive 2002/58/EC 'seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter', and, 'in particular', it 'seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter'.[16] The mention of the Charter and of its Article 8 represented a key innovation of the fundamental rights framing of the instrument, compared to its predecessor (Directive 97/56/EC), although in practice this novelty did not have any apparent impact in the Directive's construction. Like Directive 97/56/EC, Directive 2002/58/EC describes its aim as concerned with ensuring an 'equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data'.[17] Therefore, Directive 2002/58/EC perpetuated Convention 108's approach according to which the protection of personal data serves privacy, even it presented this idea surrounded with numerous joint references to the 'protection of personal data and privacy'.[18]

Directive 2002/58/EC provided a definition of the category of 'traffic data', which had already been put forward in 1997, describing it as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[19] The Directive also introduced a new category of data: 'location data', meaning 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.[20] Location data other than traffic data were granted an especially protective regime.[21] Whereas the category of traffic data could be easily ascribed to the protection of the confidentiality of communications (it was depicted as data necessary for the conveyance of communications), location data appeared to go beyond that protection, even if

[14] Similarly, the French version uses vie privée both in the heading and in the short name.

[15] Emphasis added.

[16] Recital 2 of Directive 2002/58/EC.

[17] Ibid. Article 1(1) of Directive 2002/58/EC. See also: (Martínez Martínez 2004, p. 229).

[18] See, for instance: Recitals 5, 6 and 46 of Directive 2002/58/EC.

[19] Ibid. Article 2(b). On the status of traffic data in EU law, see notably: (Pérez Asinari 2004).

[20] Ibid. Article 2(c).

[21] Ibid. Article 9.

without exactly corresponding to the notion of 'personal data'.[22] This rendered even more difficult any attempt to determine to which extent the Directive served privacy, and to which extent it was concerned with personal data protection.

In relation to traffic data, Directive 2002/58/EC built on an already existing clause[23] to establish that Member States may 'adopt legislative measures providing for the retention of data for a limited period', in the name of certain purposes such as security, defence, or crime prevention,[24] thus recognising explicitly that Member States can, in the name of these purposes, go against the basic principle according to which traffic data must be erased, or made anonymous, as soon as possible.

7.1.2.2 Directive 2006/24/EC

This possibility granted to Member States in Directive 2002/58/EC eventually resurfaced later in EU law in the shape of an obligation for Member States to impose the retention of traffic data for periods between 6 months and 2 years, in order to ensure the data's availability for the purpose of the investigation, detection and prosecution of serious crime. The obligation was concretely put forward in 2006 by a Directive formally concerned with harmonising national measures in the field: Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[25]

In line with Directive 95/46/EC, the preamble of Directive 2006/24/EC referred to Article 8 of the ECHR as establishing 'privacy' rights.[26] And, exactly like Directive 2002/58/EC, Directive 2006/24/EC presented itself as seeking to ensure compliance with both Articles 7 and 8 of the Charter.[27] There was nonetheless a manifest disconnect between the allusion to the right to personal data protection of the Charter's Article 8, and the usage of the phrase 'data protection' in the Directive's provisions: an Article of Directive 2006/24/EC titled '*Data protection*[28] and data security' dealt primarily not with anything echoing the content of Article 8 of the Charter, but rather with issues of data quality and protection against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure.[29]

---

[22] Observing it is unclear whether they are regarded by Directive 2002/58/EC as falling under the category of personal data: (Poullet 2006, p. 216).

[23] Ibid. Article 14(1).

[24] Ibid. Article 15(1).

[25] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

[26] Ibid. Recital 25.

[27] Ibid. Recital 22.

[28] Emphasis added.

[29] Article 7 of Directive 2006/24/EC.

The adoption of Directive 2006/24/EC had followed a convoluted legislative path. Initially, the proposal had been presented to the Council as a third pillar instrument (thus, as a proposal for a Framework Decision),[30] which could be adopted by consensus among all Member States. As some Member States opposed the text, it eventually re-emerged as a proposal for a Directive, which could be adopted jointly by the European Parliament and the Council without the need to have consensus in the Council. The European Parliament had expressed publicly that it rejected the very idea of imposing the retention of traffic data for law enforcement purposes,[31] but nonetheless finally backed up the proposed Directive.[32] Directive 2006/24/EC was adopted. Then, Ireland requested the European Court of Justice to annul it on the grounds that it had been adopted on an inappropriate legal basis. The ECJ, however, confirmed that the legal basis was appropriate, and dismissed the action.[33]

The boundary between the first and third pillars had already generated various inter-institutional frictions related to personal data protection. In 2006, the ECJ had annulled[34] two legal instruments adopted to allow the transfer from European private companies to US authorities of detailed personal data (Passenger Name Records (PNR) data) about travellers flying to the United States (US). The two instruments (a Council's Decision on the conclusion of the EU-US PNR agreement,[35] and

[30] Tabled as a joint proposal by four Member States: UK, France, Ireland, and Sweden.

[31] For instance, the European Parliament asserted in a 2004 Resolution that, in its view, 'Member States' laws providing for the wide-scale retention of data related to citizens' communications for law-enforcement purposes are not in full conformity with the European Convention on Human Rights' (Resolution of the European Parliament on the First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265– C5–0375/2003– 2003/2153(INI)), P5_TA(2004)0141, Strasbourg, 9.3.2004, paragraph 18). In 2005, the European Parliament rejected under the consultation procedure the proposal for a Framework Decision (European Parliament legislative Resolution on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the UK for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004– C6-0198/2004– 2004/0813(CNS)), P6_TA(2005)0348, Strasbourg, 25.9.2005).

[32] European Parliament legislative Resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438– C6-0293/2005– 2005/0182(COD)), P6_TA(2005)0512, Strasbourg, 14.12.2005.

[33] C-301/06 Ireland v *Parliament and Council* [2009] ECR I-593, Judgment of the Court (Grand Chamber) of 10 February 2009. See, on this case: (Herlin-Karnell 2009).

[34] Joined Cases C-317/04 and C-318/04 *Parliament v Council* [2006] ECR I-4721, Judgment of the Court (Grand Chamber) of 30 May 2006 ('PNR'). See, on this judgment: (González Vaqué 2006; Guild and Brouwer 2006; Pedilarco 2006; Mendez 2007; Terrasi 2008).

[35] Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection [2004] OJ L183/83, and corrigendum [2005] OJ L255/168). See, on this agreement: (Poullet and Pérez Asinari 2004).

an 'adequacy-finding' Decision of the European Commission)[36] were annulled on the grounds that the first pillar legal bases used to adopt them were inappropriate, because at stake were 'processing operations concerning public security and the activities of the State in areas of criminal law'.[37]

7.1.2.3 Framework Decision 2008/977/JHA

During the 2000s, debates among EU institutions on the protection of personal data were strongly marked by the political response to the terrorist attacks of 11 September 2001 ('9/11'). The impulsion given to EU security-related measures, and particularly to measures imposing the massive processing of personal data about both EU citizens and third-country nationals,[38] brought about numerous discussions on the eventual need to reinforce the level of (personal) data protection granted across all areas of EU law. As the Area of Freedom, Security and Justice (AFSJ) continued to be divided into two distinct pillars, measures falling under its scope were inescapably captured by asymmetrical regimes,[39] further leading to calls to bring third pillar personal data protection closer to first pillar personal data protection (which was generally governed by Directive 95/46/EC).[40] In the third pillar, the Council had the possibility to legislate without the support of the European Parliament, which repeatedly criticised the situation. For many years, the European Parliament insistently requested the adoption of a horizontal legal instrument similar to Directive 95/46/EC for the third pillar, unsuccessfully.[41] The European Parliament also

[36] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the US Bureau of Customs and Border Protection [2004] OJ L235/11.

[37] PNR § 56.

[38] See, notably: (Geyer 2008; European Commission 2010a).

[39] On the asymmetrical regimes applicable to first and third pillar large-scale information systems surfaced in the AFSJ: (Quilleré-Majzoub 2005, in particular pp. 610–611).

[40] The subject became one of the most widely debated topics in the field. Prior to the events of 9/11, the European Parliament had notably been actively investigating ECHELON, a global system for the interception of private and commercial communications. It endorsed a Resolution on the subject only a week before 9/11 (Resolution of the European Parliament on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 2001/2098(INI), 5.9.2001). There was no visible follow up to that initiative.

[41] In a Resolution adopted in 2003, the European Parliament called on the European Commission to come forward 'as soon as possible' with a binding legal instrument relating to data protection in the context of the third pillar, providing guarantees equivalent to those of Directive 95/46/EC, and requested the Council to ensure that all major EU information systems were subject to first pillar data protection (Resolution of the European Parliament on progress in 2002 in implementing an Area of Freedom, Security and Justice (Articles 2 and 39 of the EU Treaty), P5_TA(2003)0126), 27.3.2003). In March 2004, it adopted another Resolution appealing for 'a comprehensive and trans-pillar European privacy and data protection regime' (Resolution of the European Parliament of 9.3.2004, op. cit.). In June 2005, a new Resolution repeated the European Parliament's 'call for common criteria for data protection in the security domain' (Resolution of the European Parliament on progress made in 2004 in creating an Area of Freedom, Security and Justice (AFSJ) (Articles 2 and 39 of the EU Treaty), P6_TA(2005)0227, 8.6.2005).

attempted to empower data protection authorities in relation with third pillar policies, with only limited success.[42]

In the absence of any general third pillar EU instrument, Convention 108 continued to be the main reference for personal data protection in the area (Alonso Blas 2009, p. 227). This derived both from its ratification by Member States, and from the explicit references to the instrument included in specific third pillar measures. Convention 108 was for instance granted a key role in the context of the establishment of Eurojust, a EU agency dealing with judicial co-operation in criminal matters.[43] It was also mentioned by the Prüm Convention,[44] which enabled its signatories to exchange DNA data and fingerprints, signed in 2005 outside the EU institutional framework and integrated into the EU in 2008.[45]

The European Commission finally introduced a Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters in 2005 (European Commission 2005). The Council adopted the resulting Framework Decision 2008/977/JHA three years later,[46] after substantially modifying the proposal's scope of application. Whereas the original proposal by the European Commission followed an approach similar to that of Directive 95/46/EC, the Framework Decision as adopted by the Council excluded from its scope all national data processing activities. As a result of its significant limitations, Framework Decision 2008/977/JHA failed to satisfy the expectations of those who had called for the insurance of a level of protection in the third pillar at least not too dissimilar to first pillar protection (Boehm 2012, p. 114).

Council Framework Decision 2008/977/JHA, like Directive 2002/58/EC and Directive 2006/24/EC, incorporates in its preamble a joint allusion to Articles 7 and 8 of the Charter.[47] In line with Directive 95/46/EC and with Directive 2002/58/EC,

[42] See, in this sense, the amendments proposed in: European Parliament legislative Resolution of 14 November 2000 on the proposal for a European Parliament and Council regulation on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data: COM(1999) 337-C5-0149/1999-1999/0153(COD) [2001] OJ C223/73. See also: (González Fuster and Paepe 2008).

[43] See Article 14(2) of Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime [2002] OJ L63/1.

[44] Convention of 27 May 2005 between 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 on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration ('Prüm Convention'); see in particular Article 34(1), where Convention 108 is mentioned together with the Additional Protocol of 8 November 2001, and Recommendation No R (87) 15.

[45] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1, in particular Article 25(1), also referring additionally to the 2001 Additional Protocol, and Recommendation No R (87) 15.

[46] 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 [2008] OJ L350/60.

[47] Recital 48 of Council Framework Decision 2008/977/JHA.

Framework Decision 2008/977/JHA echoes in its opening provision Convention 108's approach, according to which the protection of personal data serves fundamental rights and freedoms in general, but in particular the right to privacy.[48] Contrary to those two Directives, however, the Framework Decision does not allude to any principle of free flow or free movement of personal data, although its preamble makes a reference to the 'principle of availability of information' laid down in the Council's 2004 Hague Programme.[49] The Hague Programme fixed priorities for the Area of Freedom, Security and Justice (AFSJ),[50] and described the principle of availability as the possibility for a law enforcement officer in one Member State to obtain information from another Member State.[51]

7.1.2.4 Regulation (EC) No 1049/2001

A specific joint reference to privacy and data protection in EU law eventually became source of conflicting interpretations. The controversial reference appeared in a Regulation adopted in 2001 regarding public access to documents held by the European Parliament, Council and Commission, namely Regulation (EC) No 1049/2001.[52] The Regulation, in the name of openness,[53] of transparency,[54] and of the right of public access to documents,[55] is grounded on the principle that all documents of EU institutions should be accessible to the public.[56] The Regulation lists however a series of exceptions to this principle, setting out inter alia, in its Article 4(1)(b), that EU institutions shall imperatively refuse access to a document where disclosure would undermine the protection of 'privacy and the integrity of the individual, *in particular in accordance with Community legislation regarding the protection of personal data*[57]'.[58]

Regulation No 1049/2001 did not provide any guidance on the meaning of the words privacy, integrity, the protection of personal data, or how should one interpret the notions of privacy and integrity 'in particular in accordance with' EU personal

[48] Ibid. Article 1(1).

[49] Ibid. Recital 5.

[50] Council, 'The Hague Programme: Strengthening Freedom, Security and Justice in the European Union' [2005] OJ C53/1.

[51] Ibid. 7.

[52] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [2001] OJ L145/43.

[53] As enshrined in the second subparagraph of Article 1 of the Treaty on European Union (TEU) (Recital 1 of Regulation No 1049/2001).

[54] Ibid. Recital 3.

[55] Article 255(2) of the EC Treaty (Recital 4 of Regulation No 1049/2001).

[56] Recital 11 of Regulation No 1049/2001.

[57] Emphasis added.

[58] Article 4(1)(b) of Regulation No 1049/2001 (ibid. Recital 4).

data protection.[59] Is the protection of privacy and integrity 'in particular in accordance with' EU personal data protection something different than the mere protection of privacy and integrity? If so, what is it exactly?

The Regulation's preamble solely included a vague mention of the respect of fundamental rights as laid down in the Charter of Fundamental Rights,[60] and, alluding to permissible exceptions to the general principle of accessibility of documents, declared that 'institutions should take account of the principles in Community legislation concerning the protection of personal data'.[61] This mention appears to emphasise the significance of the protection of personal data for the interpretation of the mentioned clause of Article 4(1)(b). However, another provision in the Regulation refers to that clause as an exception simply 'relating to privacy',[62] which can be interpreted as hinting that actually it is essentially about privacy, as opposed to being about personal data protection.

In comparative law it is possible to find amidst grounds accepted as valid to limit the access to public documents both references to personal data protection, and to privacy or private life. During the preparation of the draft proposal for the Regulation, a study carried out for the European Commission on national approaches argued that in Europe a majority of national legal systems provided for compulsory non-disclosure of public documents containing personal data, unless the persons concerned had given their consent. It noted also, nonetheless, that Member States also established exceptions for the respect for the private life of individuals, or other protected interests (European Commission 2000, p. 7). The study notably observed the existence of divergences between, for instance, Portugal, Greece, France or the United Kingdom (UK), which regarded as relevant criteria the identification of individuals in the documents at stake, and Sweden, where exceptions were destined to protect the 'personal integrity' of the concerned individuals (European Commission 2000, p. 7). In this light, it could be argued that the phrase 'privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data' of Article 4(1)(b) attempted to bring together the different national perspectives identified.

Controversy on the interpretation of Article 4(1)(b) of Regulation No 1049/2001 surfaced in relation to a request to access a list of participants of a meeting organised by the European Commission. The meeting had taken place in the context of infringement proceedings initiated by the European Commission against the UK, for what was called the 'guest beer provision'. This provision aimed to mitigate the effects of the common practice of UK pubs of signing exclusive contracts with beer suppliers, which de facto tied the pubs to selling beers from certain breweries. The provision stipulated that, independently of such contracts, pub owners shall always be allowed to sell some beers from other breweries.[63] These protected 'guest beers',

[59] Describing the clause as 'rather ambiguous': (Kranenborg 2008, p.1096).

[60] Recital 2 of Regulation (EC) No 1049/2001.

[61] Ibid. Recital 11.

[62] Ibid. Article 4(7).

[63] Opinion of Advocate General Sharpston in C-28/08 P *Bavarian Lager* [2010] ECR I-6055 § 39.

however, needed to comply with a series of conditions regarding their alcohol content and presentation.

For Bavarian Lager, an importer of bottled German beer into the UK,[64] the provision amounted to an obstacle to the single market, as the beers it wished to import into the UK could not benefit from the 'guest beer' exception due to their specific presentation. The European Commission investigated the issue, and found it appropriate to initiate infringement proceedings against the UK. In 1996, during the administrative procedure, a meeting was held, gathering representatives of the European Commission and of UK administrative authorities, as well as members of the Confédération des Brasseurs du Marché Commun (Confederation of Common Market Brewers). Bavarian Lager wished to attend the meeting, but was refused access. At the event, UK authorities informed the Commission that the 'guest beer provision' was to be amended. The procedure against the UK was later abandoned.[65]

Bavarian Lager then launched a series of requests to have access to the meeting's full minutes, including the participants' names. The European Commission initially refused access to such documents. In 2003, after the entry into force of Regulation No 1049/2001, Bavarian Lager introduced a new request. In 2004, the European Commission accepted to disclose some of the meeting's documents, but blanked out the names of five participants, arguing that two people had expressly objected to the disclosure of their identity, and that the other three could not be reached, and thus their consent could not be obtained.[66] Bavarian Lager brought the case to the Court of First Instance, supported by the European Data Protection Supervisor (EDPS).

The Court of First Instance ruled in 2007[67] against the European Commission's decision to refuse disclosure of some participant names. Quoting extensively the case law of the ECtHR, as well as the ECJ judgments in *Rundfunk* and *Lindqvist*,[68] the Court of First Instance maintained that the fact that the concept of 'private life' was broad could not be interpreted as meaning that it encompasses all personal data.[69] From the Court's standpoint, Article 4(1)(b) of Regulation No 1049/2001 had to be read as an exception to the principle of access to documents applicable only when the privacy and the integrity of individuals could be undermined by the processing of personal data, which is not always the case.[70] The

[64] Ibid. § 38.

[65] Ibid. § 42.

[66] Ibid. § 49.

[67] T-194/04 *Bavarian Lager Company Ltd. v Commission* [2007] ECR II-4523, Judgment of the Court of First Instance (Third Chamber) of 8 November 2007. On this judgment, see also: (Guichot 2008; Adamski 2009).

[68] T-194/04 *Bavarian Lager* § 127–129.

[69] Ibid. § 118.

[70] Ibid § 119.

information that the European Commission refused to disclose comprised names of persons acting as representatives of bodies to which they belonged. According to the Court of First Instance, that information constituted personal data, but it did not constitute personal data affecting the private life of the persons, and thus Article 4(1)(b) of Regulation No 1049/2001 was not applicable. In the Court's view, this approach did not contradict the Strasbourg case law according to which the right to respect for private life includes the right of individuals to establish and develop relations with others, and may extend to professional or business activities,[71] allegedly because such case law 'does not mean that any professional activity is wholly and necessarily covered by protection of the right to respect for private life'.[72]

The European Commission introduced an appeal against the judgment of the Court of First Instance. As a result, in 2010 the European Court of Justice ruled in its *Bavarian Lager*[73] judgment that the Court of First Instance[74] had adopted a 'particular and restrictive interpretation' of Article 4(1)(b) of Regulation No 1049/2001 that did not correspond to the intention of the EU legislator.[75] For the ECJ, the clause of Article 4(1)(b) is 'an indivisible provision' requiring that any undermining of privacy and the integrity of the individual must always be assessed in conformity with EU legislation on the protection of personal data,[76] and does not allow to separate the processing of personal data into two categories (i.e., one examined in the light of the ECHR and Strasbourg case law, and another subject to EU law).[77] Hence, the ECJ reviewed whether the European Commission had duly applied EU personal data protection provisions, found that it was the case, and ruled that the European Commission had thus been right to reject Bavarian Lager's request for full access to the minutes of the meeting.[78]

Some have interpreted *Bavarian Lager* as confirming that 'privacy underpins data protection', but advancing that the scope of EU personal data protection is broader than Article 8 of the ECHR (Oliver 2009, p. 1456). In truth, the ECJ judgment did not make any reference to Article 8 of the Charter on the protection of personal data, even though Advocate General Sharpston had expressly referred to the Article in her Opinion for the case to underline the 'fundamental importance' of the protection of personal data.[79]

---

[71] Ibid. § 130.

[72] Ibid. § 131.

[73] C-28/08 P *Commission v Bavarian Lager* [2010] ECR I-6055, Judgment of the Court (Grand Chamber) of 29 June 2010. See, on this ruling: (González Vaqué 2010).

[74] Referred to in the judgment as the General Court, its current denomination.

[75] C-28/08 P *Bavarian Lager* § 65.

[76] Ibid. § 59.

[77] Ibid. § 61.

[78] Ibid. § 79.

[79] Opinion of Advocate General Sharpston in C-28/08 P *Bavarian Lager* § 11.

7.2 Early Manifestations in the Case Law of the EU Court of Justice

It took some time for the EU Court of Justice to start mentioning the Charter in its case law. Originally invoked especially by General Advocates in their Opinions,[80] it was later also referred to by the Court of First Instance and by the ECJ (Burgorgue-Larsen 2005, p 5). At the beginning, however, the Luxembourg Court never mentioned the Charter as a source possibly diverging from the ECHR, or differing from the case law of the ECtHR, but rather as confirming and reaffirming their approaches (Burgorgue-Larsen 2005, p. 5).

In 2003, the Court of First Instance alluded to the Charter to point out that, in spite of lacking legally binding force, the instrument showed the importance for the EU of the rights it set out.[81] The ECJ first referred to the Charter in 2006,[82] in a judgment[83] concerning a Directive adopted in 2003 mentioning it in the preamble:[84] the ECJ recalled that it was bound to ensure fundamental rights as general principles of EU law, but noted the existence of the Charter[85] and stressed the Charter's linkages with previously existing sources for the identification of EU fundamental rights.

Soon after, in 2008, the ECJ referred to the Charter for the first time in a judgment related to the protection of personal data, *Promusicae*.[86] It was in this ruling where the ECJ also acknowledged for the first time the existence of a right to personal data protection.[87] The case concerned a reference for preliminary ruling on various EU provisions, questioning whether they required Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. In its answer, the ECJ examined Directive 2002/58/EC, pointing out that the Directive alluded in its

[80] Cf. Opinions of Advocate General Alber in C-340/99 TNT Traco [2001] ECR I-4109 § 94 (in reference to Article 36 of the Charter); Advocate General Tizzano in C-173/99 BECTU [2001] ECR I-4881 § 26 (in reference to Article 31(2) of the Charter); or Advocate General Léger in C-353/99 P Hautala [2001] ECR I-9565, § 51 (in reference to Article 42 of the Charter).

[81] Joined Cases T-377/00, T-379/00, T-380/00, T-260/01 and T-272/01 *Philip Morris International and Others v Commission* [2003] ECR II-1, Judgment of the Court of First Instance (Second Chamber, extended composition) of 15 January 2003, § 122.

[82] Cf. the ECtHR, which alluded to the Charter (in particular, to Article 9 on the right to marry and to found a family) in 2002, in *Christine Goodwin v the United Kingdom* [2002] ECHR 2002-VI, App. No 28957/95.

[83] C-540/03 *Parliament v Council* [2006] ECR I-5769, Judgment of the Court (Grand Chamber) of 27 June 2006.

[84] Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification [2003] OJ L251/12. See also: (Benoit-Rohmer 2011).

[85] Ibid. § 38.

[86] C-275/06 *Productores de Música España (Promusicae)* [2008] ECR I-271, Judgment of the Court (Grand Chamber) of 29 January 2008, § 64. See, on this judgment: (González Vaqué 2008; Soto García; Mari 2008).

[87] See also: (Kranenborg 2008, p. 1089). Article 8 of the Charter had been mentioned twice by Advocate General Léger in his Opinion for Case C-317/04 (on PNR): § 23, and footnote 127.

preamble to both Articles 7 and 8 of the Charter.[88] The Charter's Article 7, declared the Court, 'substantially reproduces' Article 8 of the ECHR, whereas Article 8 of the Charter 'expressly proclaims the right to protection of personal data'.[89] The Court thus innovatively used the EU Charter as a direct source for the identification of a fundamental right never before recognised as integral to the general principles of EU law (Groussot 2008, p. 1755)—and this despite the fact that, at the time, the Charter was not legally binding.

The acknowledgement of the presence of a right to personal data protection in the Charter's Article 8, however, did not have a particular impact on the reasoning of the Court in the *Promusicae* judgment. Immediately after mentioning Article 8, the Court asserted that, 'thus', the question raised by the reference for a preliminary ruling concerned the need to reconcile 'the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other'[90] (without making any further mention to the right to the protection of personal data, presumably considered subsumed under 'the right to respect for private life'). Similarly, Advocate General Kokott, in her Opinion for the case,[91] had noted the existence of the Charter's Article 8, which supposedly 'specifically emphasised the fundamental right to the protection of personal data, including important fundamental principles of data protection',[92] but had afterwards dealt with the processing of personal data in terms of an infringement of the right to respect for private life of Article 8 of the ECHR, in line with the *Rundfunk* judgment.[93]

The reference in *Promusicae* to the right to the protection of personal data did not have either any immediate effect in the subsequent case law of the ECJ. The Court continued to rule on the protection of personal data without systematically referring to the Charter, or to the new fundamental right of its Article 8. In this sense, still in 2008, the Court dealt with a reference for a preliminary ruling made in proceedings between an Austrian national, Mr Huber, and German authorities, regarding Mr Huber's requests to have data about him deleted from a German database, the Central Register of Foreign Nationals, which stored information about non-German EU citizens living in Germany. In its judgment, *Huber*,[94] the ECJ notably ruled that the database could only be regarded as compliant with Directive 95/46/EC, 'interpreted in the light of the prohibition on any discrimination on grounds of nationality', under certain strict conditions, but did not refer at all to the Charter to reach such conclusion. In his Opinion for the case, Advocate General Poiares Maduro had referred to the Charter, but only to its Article 7, allegedly

[88] *Promusicae* § 64.

[89] Ibid.

[90] *Promusicae* § 65.

[91] Opinion of Advocate General Kokott in C-275/06 *Promusicae* [2008] ECR I-271; concretely, in a Section titled 'The link between data protection and fundamental rights'.

[92] Ibid. § 51.

[93] Ibid. § 52.

[94] C-524/06 *Heinz Huber v Bundesrepublik Deutschland* [2008] ECR I-9705, Judgment of the Court (Grand Chamber) of 16 December 2008. See, notably: (González Fuster et al. 2010).

protecting 'the right to privacy' which, Poiares Maduro argued, is what 'is at stake in data protection cases'.[95]

Also in 2008, the ECJ decided on the *Satamedia* case,[96] concerning a reference for a preliminary ruling on the interpretation of Directive 95/46/EC. The case had surfaced in the context of proceedings between two Finnish companies and the Finnish Data Protection Ombudsman and Data Protection Board. The companies were Satakunnan Markkinapörssi Oy and Satamedia Oy, which collaborated to publish tax data of Finnish citizens, including details of their income and wealth, and made such data available for mobile telecommunication with the aid of a text-messaging service. The questions addressed to the ECJ notably regarded the possible qualification of the data processed as personal data, in spite of the fact that the data were in the public domain, and whether it was possible to consider the companies' activities as excluded from general data protection rules on the grounds that the activities were carried out 'for journalistic purposes'. In its answer, the Luxembourg Court underlined that it was not in dispute that 'as is apparent from Article 1', the objective of Directive 95/46/EC is to protect the fundamental rights and freedoms of individuals and, in particular, their right to privacy,[97] which needs nevertheless to be reconciled with the fundamental right to freedom of expression.[98] In her Opinion for the case, Advocate General Kokott had mentioned the existence of a specific right to the protection of personal data, enshrined in the EU Charter,[99] but nonetheless stressed that fundamental rights' issues needed to be addressed taking into account in particular the ECtHR case law.[100]

The ruling for *Rijkeboer*[101] of 2009 touched upon a key element of EU personal data protection: the right of access to personal information. The judgment concerned a reference for preliminary ruling relating to the interpretation of Directive 95/46/EC, in the context of proceedings opposing Mr Rijkeboer and the *College van burgemeester en wethouders van Rotterdam* (Board of Aldermen of Rotterdam). Mr Rijkeboer wished to obtain from the College information over the disclosure to third parties of personal data concerning him, related to the 2 years preceding his request. The College, however, gave him information only in relation with the previous year,[102] claiming that older data had been deleted in compliance with personal data protection obligations. The ECJ judged in this case without

[95] Opinion Advocate General Poiares Maduro in Case C-524/06 *Huber* [2008] ECR I-9705 § 30.

[96] C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831, Judgment of the Court (Grand Chamber) of 16 December 2008. See, notably: (Docquir 2009).

[97] Satamedia § 52.

[98] Ibid. § 53. The ECJ also ruled that the fact that the data were in the public domain was not an obstacle for their qualification as personal data, and that the notion of journalism needed to be interpreted 'broadly' § 56).

[99] Opinion of Advocate General Kokott in C-73/07 *Satamedia* [2008] ECR I-9831 § 40 (with a reference to Promusicae).

[100] Ibid. § 37.

[101] C-553/07 *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* [2009] ECR I-3889, Judgment of the Court (Third Chamber) of 7 May 2009.

[102] Ibid. § 4.

making any reference to the Charter, or to the right to the protection of personal data as such, insisting instead on the linkages between Directive 95/46/EC and the right to privacy (in the original Dutch version*, de bescherming van de persoonlijke levenssfeer*). The Court stressed that the right to privacy was mentioned in the Directive's Article 1,[103] and commented again that its importance had been highlighted in the Directive's preamble, as well as emphasised in the case law of the Court.[104] Such right to privacy, in the Court's view, notably implied that the 'data subject may be certain that his personal data are processed in a correct and lawful manner', which required that 'the basic data regarding him are accurate and that they are disclosed to authorised recipients'[105] – an idea that, as a matter of fact, echoes the content of Article 8 of the ECHR, but that the judgment expressly linked to the right of access established by Directive 95/46/EC.[106] In his Opinion for the case,[107] Advocate General Ruiz-Jarabo Colomer had argued (mentioning *Rundfunk*)[108] that the 'fundamental right to *privacy*,[109] as a general principle of Community law, had found legislative expression' in Directive 95/46/EC, 'the provisions of which were codified in Article 8 of the Charter'.[110]

7.3 Post-Lisbon: December 2009 Onwards

Soon after the proclamation of the Charter in 2000, a debate on the elaboration of a Constitution for the EU was launched (Rallo Lombarte 2003, p. 202). Following the Laeken European Council of December 2001, a second Convention was put in place to draft the text, chaired by former French President Valéry Giscard d'Estaing.[111] This Convention soon discussed the legal status of the EU Charter. Three Member States were particularly reluctant to grant to the Charter legally binding force: the United Kingdom, Ireland and, for technical reasons, the Netherlands (Jacqué 2003, p. 29). Eventually, an agreement was found allowing to give to the Charter binding force without changing its substantive provisions on rights and principles, but modifying, instead, its final clauses (Jacqué 2003, p. 29).

The final text of the draft EU Constitution was settled in June 2004. Named the draft Treaty Establishing a Constitution for Europe, it was signed in 2004 by

[103] Ibid. § 46.

[104] Ibid. § 47 (with references to *Rundfunk, Lindqvist, Promusicae*, and *Satamedia*).

[105] Ibid. § 49.

[106] Ibid. § 50.

[107] Opinion of Advocate General Ruiz-Jarabo Colomer in C-553/07 *Rijkeboer* [2009] ECR I-3889.

[108] Ibid. § 20.

[109] Emphasis added. In the original Spanish version of his Opinion: *right to intimidad*.

[110] Ibid. § 8.

[111] It was composed of two members of Parliament of each Member State and applicant country, sixteen members of the European Parliament, two members of the European Commission, and a representative from the government of each Member State.

representatives of the then twenty-five Member States. The draft Treaty included two basic provisions on the protection of personal data: one that established it as a right (Article II-68), mirroring Article 8 of the Charter (De Schutter 2005, p. 123), and another proclaiming it under Title VI, 'Of the democratic life of the Union', as one of the elements of such democratic life (Article I-51) (Murillo de la Cueva 2009, p. 67). Article I-51 of the draft Constitutional Treaty partially mirrored Article 286 of the Treaty and established the right to data protection in the general context of EU institutions,[112] allowing for the adoption of instruments not limited to the first pillar as under the mentioned Article 286 (European Commission 2007, p. 8).

The draft Constitutional Treaty required ratification by the Member States. Following its rejection by referenda in France and the Netherlands (in May and June 2005), EU leaders decided in June 2007 to set up an Intergovernmental Conference to prepare instead a Reform Treaty, which led to the adoption of the Lisbon Treaty.

7.3.1 The Lisbon Treaty

The Treaty of Lisbon[113] was signed on 13 December 2007 by the 27 Heads of State or Government of EU Member States, and came into force on 1 December 2009. It amended the two fundamental treaties, namely the Treaty on European Union (TEU), and the Treaty establishing the European Community (TEC), which became the Treaty on the Functioning of the European Union (TFEU). The entry into force of the Lisbon Treaty had an impact on EU personal data protection on a number of grounds. One of the major changes it introduced was the abolition of the pillar structure. It also modified the EU architecture for the protection of fundamental rights in general, and specifically the Treaty provisions on the protection of personal data.[114]

Since the entry into force of the Treaty of Lisbon, the major provision on fundamental rights in EU law is Article 6 of the TEU,[115] which describes the three major modes of integration of fundamental rights in the EU legal order. Article 6(3) TEU sets out that the fundamental rights said to result from the constitutional traditions common to Member States and those established by the ECHR are to be ensured as general principles of EU law. This provision thus confirms established ECJ doctrine. Article 6(2) TEU announces that the EU is to accede to the ECHR, enhancing

[112] The final content of Article I-51 of the draft Constitutional treaty was however criticised for being more limited in scope than originally foreseen (Guerrero Picó 2005, p. 293).

[113] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 [2007] OJ C306/1.

[114] On the impact of the Lisbon Treaty on EU (personal) data protection, see also: (Spiecker gen. Döhman and Eisenbarth 2011).

[115] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2010] OJ C83/1. See also Article 2 of the TEU: 'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail'.

EU's connection with the ECHR's set of rights.[116] And Article 6(1) TEU grants to the EU Charter the same legal value as the EU Treaties, supporting the applicability of the rights it guarantees throughout EU law. EU fundamental rights are thus now governed by a variety of sources, and safeguarded through a variety of mechanisms (Benoit-Rohmer 2011, p. 146). Pending the concretisation of EU's accession to the ECHR, the modified legal status of the Charter is the most important innovation brought about by the Lisbon Treaty in the area.

7.3.1.1 Modified Legal Status for the (Revised) EU Charter

The version of the Charter granted legally binding force by the Lisbon Treaty is an amended version of the 2000 Charter.[117] This amended version notably incorporates changes introduced into the Charter's final clauses already in 2003, during the negotiation of the draft Constitutional Treaty, with the view of mitigating resistance against its incorporation into the Constitution. Some of these changes have been described as 'highly problematic' (Vranes 2003, p. 1).[118] Article 52(4) of the Charter, for instance, sets out that '(i)n so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions', which does not particularly contribute to clarity, taking into account the vagueness of the obligation of interpreting rights 'in harmony' with multiple constitutional traditions.

Article 52(7) of the revised Charter establishes that the 'explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States'. This is an important novelty, as the Explanations drafted during the Convention had not been designed for such purpose.[119] The very text of the Explanations was also modified in 2007. The current version presents itself a 'a valuable tool of interpretation intended to clarify the provisions of the Charter'.[120] In relation to Article 8 of the Charter, on the protection of personal data, the current version of the Explanations incorporates a reference to Article 16 of the TFEU (noting that it replaced Article 286 of the TEC), and to Article 39 of the TEU, as well as a mention of Regulation No 45/2001, advanced as containing, together with Directive 95/46/EC, 'conditions and limitations for the exercise of the right to the protection of personal data.'[121]

[116] See also Declaration No 2 on Article 6(2) of the Treaty on European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, where the Conference noted 'the existence of a regular dialogue between the Court of Justice of the European Union and the European Court of Human Rights; such dialogue could be reinforced when the Union accedes to that Convention'.

[117] Charter of Fundamental Rights of the European Union [2010] OJ C83/389.

[118] See also: (Amato and Ziller 2007, p. 115).

[119] Ibid. A reference to the Explanation was also added to the Charter's preamble.

[120] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17.

[121] Ibid. 20.

The Lisbon Treaty did not directly incorporate the Charter into the Treaties. Article 6(1) of the TEU merely establishes that the rights, freedoms and principles set out in the Charter shall have the same legal value as the Treaties. Additionally, Article 6(1) of the TEU declares that the Charter shall not extend EU competences as defined in the Treaties,[122] and that the 'rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions' (echoing Article 52(7) of the Charter).

A Declaration annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon stresses the role of the Charter as corroborating rather than creating any new rights, by declaring that the Charter 'confirms the fundamental rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States'.[123] A Protocol similarly annexed sets out special provisions for the application of the Charter to Poland and the UK.[124]

7.3.1.2 Personal Data Protection in the Treaties

The Lisbon Treaty integrated into the EU Treaties a key new provision on the protection of personal data: Article 16 of the TFEU, technically replacing Article 286 of the EC Treaty. Article 16 of the TFEU reads:

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

---

[122] As confirmed also in Article 51(2) of the EU Charter.

[123] Declaration No 1 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007.

[124] Protocol (No 30) on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom. See also Declaration No 61 by the Republic of Poland on the Charter of Fundamental Rights of the European Union, and Declaration No 62 by the Republic of Poland concerning the Protocol on the application of the Charter of Fundamental Rights of the European Union in relation to Poland and the United Kingdom. A draft protocol to incorporate the Czech Republic to Protocol 30 was eventually proposed by the European Council.

Article 16(1) of the TFEU thus enshrines the right to the protection of personal data in almost the same terms as Article 8(1) of the Charter,[125] whereas Article 16(2) provides a new legal basis for the European Parliament and the Council to lay down rules on personal data for data processing falling under EU law, and recalls that compliance with these rules shall be subject to control by an independent authority. The mention of Article 39 of the TEU concerns personal data protection for data processed by Member States[126] when carrying out activities falling under EU's Common Foreign and Security Policy.

As a result of Article 16(2) of the TFEU, the European Parliament and the Council can legislate on data protection across EU law, applying to all EU policies (Reding 2012, p. 120), and thus irrespective of the pillar structure (which had in any case disappeared with the entry into force of the Lisbon Treaty). This allows the European Parliament and the Council, for instance, to adopt data protection rules to replace Directive 95/46/EC without any need to ground them in a legal basis on the establishment of the single market.[127] It must be noted, however, that this does not represent the disappearance of the notion of 'free flow' of personal data, which had been sustained by Directive 95/46/EC as a proof of its connection with the internal market. On the contrary, Article 16(2) of the TFEU explicitly refers to the 'free movement' of personal data, now applying not only to the internal market, but across the whole spectrum of activities falling under EU law. If Article 16 of the TFEU recognises for the first time the need for rules on data protection across all EU law (Boehm 2012, p. 116), it does so in conjunction with the enshrinement of the free movement of personal data. This linkage between the right to the protection of personal data and the free movement of personal data as enshrined in the Treaties indirectly affects the interpretation of the Charter's Article 8. Indeed, Article 52(2) of the current Charter establishes that '(r)ights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties'.[128]

Two Declarations annexed to the Lisbon Treaty relate specifically to Article 16 of the TFEU. One states that whenever are adopted rules on the protection of personal data that 'could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter'.[129] The other suggests 'specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and

[125] The only difference being the use of the pronoun 'them' (instead of 'him or her' as in the Charter). Describing this as a 'questionable alteration': (Oliver 2009, p. 1456).

[126] Only when processed by Member States (Article 29 Data Protection Working Party and Working Party on Police and Justice 2009, p. 7).

[127] For the third pillar, it replaces Articles 30 (1)(b) and 34 (2)(b) TEU.

[128] The original version of Article 52(2) was slightly different, and set out that '(r)ights recognised by this Charter which are *based on* (emphasis added) the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties'. Although it could be debatable whether Article 8 of the Charter is 'based on' Treaty recognition, it cannot be disputed that there is currently a provision on such right in the TFEU.

[129] Declaration No 20 on Article 16 of the Treaty on the Functioning of the European Union.

police cooperation (…) may prove necessary because of the specific nature of these fields'.[130]

7.3.2 Case Law of the EU Court of Justice

The EU Court of Justice, which had already referred to Article 8 of the Charter before the Charter acquired legally binding status, started to bring the provision to the fore even more regularly after December 2009. Some of the Court's judgments attempted to assemble the new right by accommodating it into previous case law, which had been marked by a strong emphasis on the connection between EU personal data protection and Article 8 of the ECHR.[131]

7.3.2.1 A Right to Respect for Private Life with Regard to the Processing of Personal Data

The judgment for *Schecke and Eifert*[132] is illustrative of this approach. It concerned a reference for a preliminary ruling on the validity of EU provisions on the publication of information relating to the beneficiaries of EU agricultural funds, and on the interpretation of Directive 95/46/EC. The reference had surfaced in the course of proceedings between the recipients of EU funds Volker und Markus Schecke GbR and Mr Eifert, on the one hand, and the German federal state of Hesse, on the other.

The ECJ, noting that Article 6(1) of the TEU gives to the Charter the same legal value as the Treaties,[133] declared that the validity of the provisions at stake had to be assessed in the light of the Charter[134] and that, in this regard, Article 8(1) of the Charter states that everyone has the right to the protection of personal data.[135] The Court added that the fundamental right to the protection of personal data is closely connected to the right to respect for private life expressed by Article 7 of the Charter.[136] From there, the ECJ moved to asserting that the right to the protection of personal data is not an absolute right,[137] and, in this context, noted that Article 8(2)

[130] Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation. Viewing these Declarations as an open door for the adoption of specific rules in these areas despite the existence of a single legal basis in Article 16 TFEU: (Boehm 2012, p. 117).

[131] See, on this case law: (González Fuster and Gellert 2012).

[132] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, Judgment of the Court (Grand Chamber) of 9 November 2010.

[133] *Schecke and Eifert* § 45.

[134] Ibid. § 46.

[135] Ibid. § 47.

[136] Ibid.

[137] Ibid. § 48.

of the Charter authorises the processing of personal data under some conditions,[138] that Article 52(1) of the Charter accepts some limitations to the rights set forth in Articles 7 and 8 of the Charter,[139] and that, according to Article 52(3) of the Charter, insofar as the Charter contains rights corresponding to the ECHR, they must be similarly interpreted.[140] Taking into account all this, the ECJ put forward the existence of a 'right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter', the content of which was described with references to ECtHR case law.[141] This right, the Court pointed out, can be lawfully limited if under the conditions established by Article 8(2) of the ECHR.[142] In the end, the Court assessed whether the measures at stake could be regarded as an interference with Articles 7 and 8 of the Charter and, having concluded that they did, it went on to examine whether the interference was justified having regard to Article 52(1) of the Charter.[143]

The *Schecke and Eifert* judgment thus exemplifies a will to adjudicate on the basis of the Charter,[144] while at the same time making use of the ECHR and of the case law of the ECtHR. To combine the two perspectives, the ECJ takes a series of peculiar shortcuts. Notably, it assimilates Article 7 and 8 of the Charter to create an unprecedented right, the 'right to respect for private life with regard to the processing of personal data', and it portrays the right to the protection of personal data as being set forth by Article 8(1) of the Charter (instead of the complete Article 8), allowing it to present as parallel provisions Article 8(2) of the Charter, Article 52(1) of the Charter, and Article 8(2) of the ECHR. In her Opinion on the Case,[145] Advocate General Sharpston had observed that two rights had been invoked, a 'classic' right to privacy under Article 8 of the ECHR, and a more modern right, described as 'data protection' under Convention 108. The Advocate General asserted that these rights were similar to those identified in Articles 7 and 8 of the Charter, and noted that the ECJ had recognised a close link between the two rights,[146] but she did not grant any particular relevance to their specificities, graphically referring to the fact that the applicants enjoyed a right 'to privacy and/or to the protection of personal data'.[147]

---

[138] Ibid. § 49.

[139] Ibid. § 50.

[140] Ibid. § 51. Regarding this as a combined application of the Charter and the ECHR: (Benoit-Rohmer 2011, p. 161).

[141] Concretely, to *Amann* and *Rotaru*.

[142] *Schecke and Eifert* § 52.

[143] Ibid. § 69. This allowed the Court to assert that the measures pursued a legitimate purpose, namely transparency, regarded as an objective of general interest recognised by the EU (§ 71), even if the Court considered that they did not comply with proportionality requirements.

[144] Even despite the fact that the case referred to events occurred in September 2008 (Lind and Strand 2011, p. 4).

[145] Opinion of Advocate General Sharpston in Joined Cases C-92/09 and C-93/09 *Schecke and Eifert* [2010] ECR I-11063.

[146] Ibid. § 71 (referring notably to *Promusicae* and to the Opinion of Advocate General Ruiz Jarabo Colomer in *Rijkeboer*, as well as to Directive 95/46/EC).

[147] Ibid. § 65.

The finding in *Schecke and Eifert* of a 'right to respect for private life with regard to the processing of personal data' jointly recognised by Articles 7 and 8 of the Charter was echoed in a judgment of November 2011, *ASNEF and FECEMD*.[148] Here the Luxembourg Court had to deal with a reference for a preliminary ruling on the interpretation of Directive 95/46/EC, concretely on whether the Directive allowed to condition the processing of personal data undertaken to pursue a legitimate interest of the data controller (or of a third party), in the absence of the consent of the data subject, to the requirement that the data should appear in publicly available sources.[149] In its ruling, the Court systematically alluded to Articles 7 and 8 of the Charter together.[150] It reproduced the assertions according to which the right to the protection of personal data is enshrined by Article 8(1) of the Charter, which is 'closely connected' to Article 7 of the Charter,[151] and affirmed that the right jointly recognised by Articles 7 and 8 of the Charter can be restricted under the conditions set forth by Article 8(2) and 52(1) of the Charter.[152]

7.3.2.2 The Charter and its Article 8 as Main Reference

A more straightforward incorporation of the right to personal data protection in the case law of the EU Court of Justice saw the light in two judgments dealing with the fight against piracy on the Internet.[153]

In *Scarlet*,[154] the Court had to deal with a reference for preliminary ruling on the interpretation of two Directives relating to the protection of intellectual property,[155] a Directive on electronic commerce,[156] and Directives 95/46/EC and 2002/58/EC. The facts in the main proceedings concerned an injunction sought by the Société belge des auteurs compositeurs et éditeurs (SABAM) against Scarlet

[148] Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD)* (C-469/10) v Administración del Estado, Judgment of the Court (Third Chamber) of 24 November 2011, not yet published.

[149] The ECJ found that Article 7(f) of Directive 95/46/EC must be interpreted as precluding the existence of national rules with that effect.

[150] *FECEMD and ASNEF* § 40.

[151] Ibid. § 41.

[152] Ibid. 42.

[153] On this subject, see also: (González Fuster 2012).

[154] C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgment of the Court (Third Chamber) of 24 November 2011, not yet published.

[155] Directive of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10; Directive of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L157/45; corrections: [2004] OJ L195/16, and [2007] OJ L204/27.

[156] Directive of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1.

Extended SA, an Internet Service Provider (ISP), to force this company to implement a system for filtering and blocking electronic communications. The national court that had introduced the reference for preliminary ruling had inquired about the interpretation of EU law in the light of Articles 8 and 10 of the ECHR, respectively on the right to respect for private life and freedom of expression. In his Opinion for the Case, Advocate General Cruz Villalón proposed to the EU Court of Justice to reformulate the question as inquiring about an interpretation of EU law in the light of 'Articles 7, 8 and 11 of the Charter, in conjunction with Article 52(1) thereof, as interpreted, in so far as necessary, in the light of Articles 8 and 10 of the ECHR'.[157] Cruz Villalón grounded the suggestion on the fact the post-Lisbon legal status of the Charter made the recourse to identification of fundamental rights as general principles (and thus in reference to the ECHR) 'no longer necessary'.[158] Nonetheless, the Advocate General noted that Article 52(3) of the Charter requires that Charter rights corresponding to ECHR rights shall be interpreted similarly, and he pointed out that Article 10 of the ECHR 'corresponds' to Article 11 of the Charter, whereas, he suggested, Article 8 of the ECHR 'corresponds' to Articles 7 and 8 of the Charter.[159] Regarding permissible restrictions, Cruz Villalón observed that in ECHR the requirements for legitimate interferences were described in Articles 8(2) and 10(2), whereas the Charter described lawful limitations in Article 52(1). He stressed that these provisions were equivalent 'to a large extent', but that, to the extent that they differ, the provisions of the Charter shall be given 'an independent interpretation'.[160] The Advocate General's Opinion advanced the idea that Directives 95/46/EC and 2002/58/EC must be primarily interpreted having regard to Articles 7 and 8 of the Charter,[161] 'construed if appropriate in the light of Article 8 of the ECHR'.[162] He thus granted to the Charter a privileged role for the interpretation of EU data protection laws (displacing the ECHR), even though he did not link these laws solely to the right to the protection of personal data, but rather to both the right to respect for private life, and to the protection of personal data.

In its judgment for *Scarlet*, the Court did not even mention Article7 of the Charter, or Article 8 of the ECHR. It did not refer to privacy, or to the right to respect for private life. The Luxembourg Court focused its analysis on the fact that the measure at stake pursued the protection of the right to intellectual property,[163] and recalled that *Promusicae* had stressed that the protection of the rights linked to intellectual

[157] Opinion of Advocate General Cruz Villalón in Case C-70/10 *Scarlet*, delivered on 14 April 2011, § 34.

[158] Ibid. § 30. See also: Benoit-Rohmer (2011) op. cit. 160.

[159] Opinion of Advocate General Cruz Villalón in *Scarlet*, § 31.

[160] Ibid. § 33.

[161] An idea that Cruz Villalón supported referring to *Rundfunk, Satamedia*, and *Schecke and Eifert*, as well as the Opinion of Advocate General Kokott in *Promusicae*.

[162] Ibid. § 73.

[163] *Scarlet* § 43.

property must be balanced against the protection of other fundamental rights,[164] concretely the fundamental rights of individuals who are affected by such measures.[165] The Court asserted that the individuals affected by the measure at stake included notably ISP customers,[166] because the system for filtering and blocking electronic communications would infringe their right to protection of their personal data, and their freedom to receive or impart information, 'rights safeguarded by Articles 8 and 11 of the Charter respectively'.[167] The assertion that the right to the protection of personal data of Article 8 of the Charter was affected was exclusively grounded on the fact that the injunction at stake would involve a systematic processing of IP addresses, and that IP addresses were described as allowing the precise identification of users, and, thus, as constituting personal data.[168]

The reasoning in *Scarlet* was later reproduced in *Netlog*,[169] concerning a reference for a preliminary ruling in the context of proceedings opposing SABAM and Netlog, owner of an online social networking platform, also in relation to a possible injunction for the introduction of a system for filtering information. In this judgment, the Court observed that the measure would involve the systematic processing of information connected with users' profiles, profiles to be regarded as personal data,[170] and inferred from this idea that, in adopting an injunction requiring Netlog to install the contested filtering system, the national court would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the right personal data protection, on the other.[171]

Not all post-Lisbon judgments of the EU Court of Justice on the protection of personal data have included references to the fundamental right to the protection of personal data. In March 2010, the Luxembourg Court ruled in *Commission v Germany* on the independence of data protection authorities,[172] which is an element

[164] Ibid. § 44.

[165] Ibid. § 45. This idea was also echoed in C-461/10 *Bonnier Audio and Others* (Judgment of the Court (Third Chamber) of 19 April 2012, not yet published § 49), where nonetheless the EU Court of Justice failed to identify the applicable fundamental rights to be balanced. Similarly mentioning a need to balance 'the various fundamental rights involved', whithout naming them: C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* [2009] ECR I-1227, Order of the Court (Eighth Chamber) of 19 February 2009.

[166] The ECJ also observed that measures such as the contested affected the freedom to conduct a business enjoyed by operators (ibid. § 46).

[167] Ibid. § 50.

[168] Ibid. § 51.

[169] C360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV,* Judgment of the Court (Third Chamber) of 16 February 2012, not yet published.

[170] Ibid. § 49.

[171] Ibid. § 51 (referring 'by analogy' to *Scarlet*).

[172] C-518/07 *Commission v Germany* [2010] ECR I-1885, Judgment of the Court (Grand Chamber) of 9 March 2010. An action had been brought by the European Commission asking the ECJ to declare that Germany had failed to correctly implement Directive 95/46/EC because it did not ensure the complete independence of data protection authorities established at Länder level, and responsible for monitoring the processing of personal data outside the public sector. The Luxembourg Court agreed that Germany had failed to fulfil its obligations.

explicitly present in Article 8 of the Charter, but it failed to make any allusion to the instrument.[173] In contrast, in a similar ruling of October 2012, *Commission v Austria*,[174] this time concerning the independence of the Austrian data protection authority,[175] the Court found it appropriate to note that the requirement that compliance with EU rules on the protection of individuals with regard to the processing of personal data is subject to control by an independent authority 'derives from the primary law of the European Union, inter alia Article 8(3) of the Charter of Fundamental Rights of the European Union and Article 16(2) TFEU'.[176]

7.3.2.3 Directive 95/46/EC Serves the Protection of Personal Data

In a judgment of May 2011, the Luxembourg Court asserted for the first time that the purpose of Directive 95/46/EC is the insurance of the right to personal data protection. The case, *Deutsche Telekom*,[177] concerned a reference for a preliminary ruling on the interpretation of a Directive on electronic communications networks and services,[178] and Directive 2002/58/EC, in the context of proceedings about the obligations of undertakings assigning telephone numbers to make available to certain parties (including to competitors) data related to subscribers. In its judgment, the Court remarked that Directive 2002/58/EC 'clarifies and supplements' Directive 95/46/EC,[179] and recalled that Article 1(1) of the latter states that it is 'aimed at protecting the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data',[180] but nevertheless declared that Directive 95/46/EC 'is designed to ensure, in the Member States, observance of the right to protection of personal data'.[181]

The ECJ thus interpreted Directive 2002/58/EC[182] in the light of the right to the protection of personal data, which it identified as enshrined in the Charter's

[173] Advocate General Mazák did not mention the Charter in his Opinion for the case (which notably proposed to the ECJ to dismiss the action) (Opinion of Advocate General Mazák in C-518/07 *Commission v Germany*, delivered on 22 October 2009).

[174] C-614/10 *Commission v Austria*, Judgment of the Court (Grand Chamber) of 16 October 2012, not yet published.

[175] Resulting from a complaint submitted to the European Commission in 2003 by the Austrian organisation ARGE DATEN.

[176] *Commission v Austria* § 36.

[177] C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* [2011] ECR I-3441, Judgment of the Court (Third Chamber) of 5 May 2011.

[178] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [2002] OJ L108/51.

[179] *Deutsche Telekom* § 50.

[180] Ibid. § 3.

[181] Ibid. § 50.

[182] That it routinely referred to in the German authentic version of the judgment using its official short name: *Datenschutzrichtlinie für elektronische Kommunikation* ('Data protection Directive for electronic communications').

Article 8(1).[183] Following *Schecke and Eifert*, the Court stressed that this right is not absolute,[184] and noted that 'Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied'.[185] The Court, therefore, depicted Directive 95/46/EC as serving the right to protection of personal data, but put forward a construction of the right as enshrined by Article 8(1) of the Charter, and potentially lawfully limited under Article 8(2) of the Charter (and regardless of Article 52 of the Charter, a provision which was not mentioned). It eventually concluded that Directive 2002/58/EC did not prohibit the existence of national laws imposing some transfers of data from telephone service providers to some third parties active in the publication of directories, as long as the subscribes are informed before the inclusion of their data in the directory, and that the data are not used for other purposes.

The EU Court of Justice also alluded to the fact that the protection of personal data is 'provided for in Article 8 of the Charter' in a judgment of July 2011 on access to documents and the burden of proof in discrimination cases, *Patrick Kelly*.[186] Here, the Court referred to Directives 95/46/EC and 2002/58/EC as rules of EU law 'relating to confidentiality' that can affect the entitlement to access to some documents.[187]

7.3.3 The 2012 Legislative Package

Directive 95/46/EC obliged the European Commission to regularly report to the Council and the European Parliament on the Directive's implementation, attaching to the report, 'if necessary, suitable proposals for amendments'.[188] In its first report, published in 2003, the European Commission stated first of all that Directive 95/46/EC enshrined 'two of the oldest ambitions of the European integration project: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals' (European Commission 2003). In this sense, the Commission argued that, although the Directive's adoption rested legally on internal market grounds, the proclamation in 2000 of the Charter, and in particular of its Article 8 incorporating 'the right to *data protection*[189]', had given added emphasis to the Directive's fundamental rights dimension (European Commission 2003, p. 4). The 2003 Communication reviewed the status of implementation of Directive 95/46/EC, and

[183] *Deutsche Telekom* § 49.

[184] Ibid. § 51.

[185] Ibid. § 52.

[186] C-104/10 *Patrick Kelly v National University of Ireland* (University College, Dublin), Judgment of the Court (Second Chamber) of 21 July 2011, not yet published, § 55.

[187] Ibid. § 56.

[188] Article 33 of Directive 95/46/EC.

[189] Emphasis added. The European Commission also alluded to individuals' 'data protection rights' (European Commission 2003, p. 20).

concluded that no legislative changes were needed, but that work had to be done to improve the situation. For this purpose, the report contained a 'Work Programme for better implementation of the Data Protection Directive', which notably included an Action on the promotion of Privacy Enhancing Technologies (PETs) (European Commission 2003, p. 23).

In 2007, the European Commission issued a Communication on the follow-up to the 2003 Work Programme. In this 2007 Communication, the Commission expressed that Directive 95/46/EC had 'set a milestone in the history of the protection of personal data as a fundamental right, down the path paved by Council of Europe Convention 108' (European Commission 2007, p. 2). It even manifested that the Directive actually 'gives shape to the fundamental right to protection of personal data' (European Commission 2007, p. 9). The Commission alluded repeatedly to Article 8 of the Charter, here always presented as enshrining a right 'to the protection of personal data' (instead of 'to data protection'),[190] even if it also took the view that Directive 95/46/EC should serve as a point of reference on 'the respect for privacy' (European Commission 2007, p. 8). The main message of the 2007 Communication was that the Commission still did not envisage submitting any legislative proposal to amend the Directive (European Commission 2007, p. 9). After the signature of the Lisbon Treaty in December of 2007, the Commission's view finally changed.

In May 2009, the European Commission launched a public consultation about the future legal framework for the fundamental right to the protection of personal data in the EU.[191] In June, it published a Communication on the Area of Freedom, Security and Justice (AFSJ) with a section on 'Promoting citizens' rights: a Europe of rights', which included a sub-section on the 'Protection of personal data and privacy'. Here, the Commission argued that the EU had to 'respond to the challenge posed by the increasing exchange of personal data and the need for utmost respect for the protection of privacy' (European Commission 2009, pp. 7 and 8). In this context, and referring to both the rights to privacy and to the protection of personal data guaranteed by the Charter. the Commission suggested that '(i)n the light of the speed of technological change, further legislative or non-legislative initiatives may be necessary' (European Commission 2009, p. 8). The consultation launched in May 2009 was over by December 2009, and was followed by a series of targeted stakeholders' consultations.

In November 2010, the European Commission published a new Communication, announcing now its intention to propose, in 2011, legislation aimed at revising the EU legal framework for data protection (European Commission 2010c, p. 18). In this document, the Commission reproduced the opening statement of its 2003 Com-

[190] See, for instance: (European Commission 2007, pp. 2 and 8).

[191] Which notably included the celebration of a Conference titled 'Personal data—more use, more protection?' in Brussels, on 19 May 2009. During the event was distributed merchandising (including pens, and sticky notes) with the slogan 'The protection of your personal data is your fundamental right'. The consultation notably asked for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation.

munication, but slightly altered: now it asserted that Directive 95/46/EC 'enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals *and in particular the fundamental right to data protection*,[192] on the one hand, and the achievement of the internal market –the free flow of personal data in this case– on the other' (European Commission 2010c, p. 2).[193] In contrast with its 2007 Communication, the Commission now alluded to the right established in Article 8 of the Charter sometimes as the right 'to the protection of personal data' (European Commission 2010c, 4 and 5), and others as a right 'to data protection' (European Commission 2010c, pp. 2, 4 and 5). References to privacy appeared mainly in the context of concrete concepts or mechanisms to be explored, such as 'privacy by design', 'privacy seals', or 'privacy-compliant' processes (European Commission 2010c, p. 12).

7.3.3.1 Privacy (Almost) Gone

The announced legislative package was published by the European Commission in January 2012. It consists of a proposal for a *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (European Commission 2012a), intended to replace Directive 95/46/EC, and a proposal for a *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* (European Commission 2012b), designed to replace Framework Decision 2008/977/JHA16. The proposed Regulation would be directly applicable in all Member States (European Commission 2012c, p. 8).

The proposals were accompanied by a Communication, titled *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*. In this document, the European Commission advanced the protection of personal data as concerned with ensuring that individuals have the right to enjoy effective control over their personal information (European Commission 2012c, p. 2).[194] It presented the main innovations put forward by its proposals, such as the introduction of a right to be forgotten, and a right to data portability; the encouragement of the use of privacy-enhancing technologies (described as 'technologies which protect the privacy of information'), privacy-friendly default settings and

[192] Emphasis added.

[193] The sentence, with some changes in punctuation, was signed by Commissioner Viviane Reding (Commissioner responsible for Justice, Fundamental Rights and Citizenship since 2010) in 2012 (Reding 2012, p. 120).

[194] See also the section 'Putting individuals in control of their personal data' (European Commission 2012c, p. 4).

privacy certification schemes; a general obligation to notify data breaches;[195] an obligation to designate data protection officers in some cases; the introduction of the 'privacy by design' principle, and the obligation to carry out data protection impact assessments in some circumstances; the transformation of Article 29 Working Party into a European Data Protection Board; or a clarification of applicable rules (European Commission 2012c, pp. 6–7, 9 and 11). The reference to privacy in the Communication's title, and in its numerous occurrences in the text, contrasts with its almost complete disappearance in the proposals themselves.

The proposals introduced by the European Commission are based on Article 16(2) of the TFEU, and pivot around the right to the protection of personal data. Article 1(2) of the proposed Regulation asserts: 'This Regulation protects the fundamental rights and freedoms of natural persons, and *in particular their right to the protection of personal data*[196]' (European Commission 2012a, 40).[197] Article 1 of the proposed Directive defines its object as 'protecting the fundamental rights and freedoms of natural persons and *in particular their right to the protection of personal data*[198]'.[199] The idea of EU personal data protection law serving notably, among all fundamental rights and freedoms, the right to privacy, has thus been replaced with the assertion that it develops in particular the right to the protection of personal data. This right is not mentioned here in conjunction with the right to privacy, or as an element of privacy,[200] but in place of the right to privacy.

The Explanatory Memorandum introducing the proposal for a Regulation maintains that in 1995 the EC legislator adopted Directive 95/46EC having already 'in mind' as one of its objectives 'to protect the fundamental right to data protection' (European Commission 2012a, p. 1).[201] The Regulation's Explanatory

[195] The notification of data breaches was first incorporated into EU law through a revision of Directive 2002/58/EC undertaken in 2009 (and, thus, applying only to the electronic communications sector); see: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11. On this subject, see, notably: (Barceló and Traung 2010).

[196] Emphasis added.

[197] This formula is also echoed by Recitals 2, 7 and 129 of the proposed Regulation (European Commission 2012a, pp. 17, 18 and 37).

[198] Emphasis added.

[199] As well as ensuring that the exchange of personal data by competent authorities in the EU is not restricted for reasons connected with the protection of individuals with regard to the processing of personal data (European Commission 2012b, p. 26).

[200] As argued by the reading of the EU Agency for Fundamental Rights (FRA), which stresses in its assessment of the 2012 legislative package that Article 8 of the Charter is closely connected to 'the right to privacy as guaranteed by Article 7 of the Charter on the respect for private and family life' (EU Agency for Fundamental Rights 2012).

[201] The Explanatory Memorandum also refers to the fundamental right to personal data protection in (European Commission 2012a, pp. 2 and 6).

Memorandum expressly locates the formulation of the right to personal data protection in the Charter's Article 8, but does not present this right as completely separate from the right to respect for private life, as it stresses that '(d)ata protection is closely linked to respect for private and family life protected by Article 7 of the Charter', and that this is reflected in Article 1(1) of Directive 95/46/EC (European Commission 2012a, p. 7). In contrast, the proposed Regulation itself refers to the protection of personal data not as being enshrined by Article 8 of the Charter as such, but, instead, by the Charter's Article 8(1), and does so in the Regulation very first recital (European Commission 2012a, p. 17). The proposed Regulation also alludes to the objectives of Directive 95/46/EC, but never to the fact that the instrument established an explicit link between its objectives and the right to privacy.[202]

The displacement of privacy by personal data protection in the proposed legislative package has also affected other potential occurrences of the word. In this sense, the notion previously known as 'privacy by design' has been supplanted by 'data protection by design'. Similarly, there is no mention of any 'privacy impact assessments', but rather of 'data protection impact assessments'.[203] There is no allusion anymore to Convention 108 (Article 29 Data Protection Working Party 2012, p. 5), an instrument which famously refers to privacy in its text. And whereas Article 8(2) of the ECHR was the clear reference for the drawing of exemptions and restrictions in Directive 95/46/EC, now the issue is less clear.[204] As a matter of fact, the proposed Regulation appears to hesitate between competing conceptions of what constitutes a limitation to the fundamental right to personal data protection:[205] it echoes (even if only partially) the wording of Article 8(2) of the ECHR and of Article 52(1) of the Charter both when addressing restrictions to the general rules of the proposed Regulation,[206] and when describing grounds justifying the processing of personal data,[207] as if the mere processing of personal data amounted, by itself, to a limitation of the fundamental right to personal data protection.

The removal of privacy is nonetheless almost complete. Remaining allusions prove that the role foreseen for privacy is now strictly minor. The right to respect

[202] See, in this sense, Recital 7 of the proposed Regulation: 'The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data (emphasis added) afforded in the Member States may prevent the free flow of personal data throughout the Union' (European Commission 2012a, p. 18); cf. Article 1(1) of Directive 95/46/EC: 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' (emphasis added).

[203] As already foreseen by (European Commission 2010c, p. 12) and in (European Commission 2012c, p. 7).

[204] On this subject, see for instance: (González Fuster 2013).

[205] See also: (González Fuster and Gutwirth 2013).

[206] Article 22 of the proposed Regulation.

[207] Article 6(3) of the proposed Regulation.

for private and family life is for instance mentioned in the preamble of the proposed Directive as one of all the Charter's rights and principles that it respects, but only at the same level as, for instance, the freedom to conduct a business, or linguistic diversity (European Commission 2012b, p. 25).

In the proposed Regulation, a reference to privacy can be found in a Recital about 'sensitive data', which actually advances privacy as something different from fundamental rights stating that data which are, by their nature, 'particularly sensitive and vulnerable in relation to fundamental rights *or privacy*[208]' deserve specific protection.[209] A provision on personal data breaches imposes the communication to data subjects of data breaches 'likely to adversely affect the protection of the personal data *or privacy*[210] of the data subject',[211] defined in the preamble as breaches that could result in identity theft or fraud, physical harm, significant humiliation or damage to reputation.[212] In the English version of the proposed Regulation, there is still another reference to privacy, in a provision establishing that the European Commission shall be empowered to adopt delegated acts related to the security of processing taking into account 'solutions for privacy by design and data protection by default'.[213] This is however an abnormality of the English text (and of versions seemingly written as translations of the English text),[214] as other linguistic versions omit any references to equivalent notions even in that provision.[215]

7.3.3.2 Enter a (New?) Right

The right to be forgotten is one of the elements advanced in the 2012 legislative package that has generated more controversy. In 2010, the European Commission had defined it as 'the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes' (European Commission 2010c, p. 8). The proposed Regulation attaches it to a right 'to erasure'. A proposed Article advances together these two rights,[216] jointly envisaged as granting individuals the possibility to obtain, from those responsible for the processing of data about them, the erasure of such data (which would seemingly correspond

[208] Emphasis added.

[209] Recital 41 of the proposed Regulation (European Commission 2012a, 24).

[210] Emphasis added.

[211] Article 32(1) of the proposed Regulation (European Commission 2012a, p. 61).

[212] Recital 67 of the proposed Regulation (European Commission 2012a, p. 28).

[213] Article 30(3) of the proposed Regulation (European Commission 2012a, p. 60).

[214] Such as the Dutch version, which alludes to 'oplossingen inzake privacy by design en gegevens-bescherming by default'; or the Spanish version: 'soluciones de privacidad desde el diseño y la protección de datos por defecto'.

[215] The French version refers to: 'des solutions de protection des données dès la conception ainsi que par défaut'; in German: 'Lösungen für einen Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen'; Italian: 'soluzioni per la protezione fin dalla progettazione e per la protezione di default'.

[216] Article 17 of the proposed Regulation.

to the right to erasure), and the 'abstention from further dissemination', especially in relation to data made available as they were children (European Commission 2012a, p. 51). This is seemingly what is to be regarded as the 'right to be forgotten'. This right would furthermore include an obligation for those responsible for the processing of data, in case they had previously made the data public, to request that they are not further replicated, or further made accessible through links (European Commission 2012a, p. 51)—an obligation that the preamble of the proposed Regulation describes as an extension of the right to erasure serving the strengthening of the right to be forgotten.[217]

Some European countries have been discussing related mechanisms for already a few years. The French version of the proposed Regulation refers to the right to be forgotten as the *droit à l'oubli numérique* (or 'right to digital forgetfulness', or 'digital oblivion'), corresponding to the terminology previously endorsed by French authorities for soft-law instruments promoted in the area,[218] and hereby integrating, in the French version of the proposed Regulation, an explicit linkage between the right to be forgotten and automated data processing (and non-processing). In France, the *droit à l'oubli* (without the adjective *numérique*) has traditionally been used to refer to the possibility for individuals to make sure that past criminal convictions are not made publicly known.[219]

The Spanish version of the proposed Regulation incorporates the expression *derecho al olvido*, a notion under which the Spanish data protection supervisory authority, the Agencia Española de Protección de Datos (AEPD), has been during the recent years actively addressing the obligations of search engine providers in relation to the personal data they process.[220] A decision of the AEPD, which obliged search engine provider Google to stop displaying certain results, was contested by the company; the conflict eventually reached the Spanish *Audiencia Nacional*, which submitted to the EU Court of Justice a reference for preliminary ruling on the applicable norms, asking specifically for an interpretation of Directive 95/46/EC in the light of Article 8 of the Charter[221] (still pending).

The literature and EU institutions appear somehow divided on how to envisage the right to be forgotten, or whether it deserves to be envisaged at all. The European Data Protection Supervisor (EDPS) initially welcomed the right as a concept connected to data portability, describing both of them as 'new notions' (European Data Protection Supervisor (EDPS) 2011, p. 11). The EDPS portrayed data portability as giving more control to individuals on their information by ensuring that they are able to easily change service providers, and the right to be forgotten as guaranteeing the automatic deletion of personal data stored after a certain amount of time, a 'sort

[217] Recital 54 of the Proposed Regulation.

[218] In particular: Secrétariat d'Etat à la Prospective et au Développement de l'économie numérique, Charte du droit à l'oubli dans les sites collaborateurs et les moteurs de recherche and Charte du Droit à l'oubli numérique dans la publicité ciblée, both of 2010.

[219] Comparing the *droit à l'oubli* and the right to be forgotten: (Ambrose and Ausloos 2013).

[220] See, notably: (Rallo Lombarte 2010, p. 104).

[221] Case C-131/12, *Google Spain and Google*, case in progress.

of expiration date' marked in data (European Data Protection Supervisor (EDPS) 2011, p. 11).[222]

Some have argued that the right to be forgotten, although 'an attractive concept', might be 'difficult to achieve' given the nature of technologies 'which delete but do not forget'.[223] Others, on the contrary, picture it as 'the biggest threat to free speech on the Internet in the coming decade' (Rosen 2012, p. 88). Divergences are significant also in relation to the conceptualisation of the right, which has notably been described as a meta-right, surfacing not inside but beyond both the rights to privacy and personal data protection (Rouvroy and Berns 2010, p. 101).

7.4 Summary

This chapter has reviewed the integration and gradual advent of the EU fundamental right to the protection of personal data in EU law after the proclamation of the Charter of Fundamental Rights of the EU in 2000. It has addressed these developments as configuring two distinct phases: one during which the Charter had no legally binding force, and the other starting with the entry into force of the Lisbon Treaty in December 2009.

Between 2000 and 2009, EU law accommodated the appearance of a provision in the Charter alluding to a right to the protection of personal data essentially by recognising its existence only in conjunction with references to privacy. During this period, a number of joint allusions to the Charter's Article 7 and Article 8, and to 'data protection' and 'privacy', were added into legislative proposals. The entanglement of these notions, and, more precisely, the apparent ambivalence of their relationship, became eventually problematic, leading notably to the *Bavarian Lager* judgment of the European Court of Justice, where a distinction between them was advanced.

A mention of Article 8 of the Charter in the preamble to Directive 2002/58/EC allowed the ECJ to refer to this provision already in 2008, in *Promusicae*. When the Lisbon Treaty gave to the Charter the same legal value as the Treaties, the ECJ started to increasingly address the interpretation of EU personal data protection laws in the light of the Charter. The Luxembourg Court's case law, however, is still marked by its traditional support of the existence of a strong linkage between personal data protection and the right to privacy (following the *Rundfunk* line). The Court has only very rarely dealt with the protection of personal data, in its fundamental rights dimension, without referring to Article 8 of the ECHR and to the case law of the ECtHR thereof.

[222] The conception of digital forgetting as an expiration date for information had actually been supported previously in the literature: (Mayer-Schönberg 2009, using the expression "expiration date": p. 15).

[223] Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—A comprehensive approach on personal data protection in the European Union COM(2010) 609 final, [2011] OJ C248/123, p. 126.

The legislative package for the future of EU personal data protection presented by the European Commission in January 2012 seemingly signals a key change in its fundamental rights framing. It heralds the abandonment of the Convention 108 formula, which had been consolidated by Directive 95/46/EC, according to which the protection of personal data serves fundamental rights and freedoms in general, but in particular privacy. It retains the structure of this formula, but replaces the reference to privacy with a mention of the right to the protection of personal data. It also puts on the table the possible recognition of a new mechanism of protection, designated as the right to be forgotten.

References

Adamski, Dariusz. 2009. How wide is 'the widest possible'? Judicial interpretation of the exceptions to the right of access to official documents revisited. *Common Market Law Review* 46:521–549.

Alonso Blas, Diana. 2009. First pillar and third pillar: Need for a common approach on data protection? In *Reinventing Data Protection?* eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak. Nouwt, 225–237. Dordrecht: Springer.

Amato, Giuliano, and Jacques Ziller. 2007. *The European Constitution: Cases and Materials in EU and Member States' Law*. Cheltenham: Edward Elgar.

Ambrose, Meg Leta, and Ausloos, Jef. 2013. The right to be forgotten across the pond. *Journal of Information Policy* 3:1–23.

Article 29 Data Protection Working Party. 2007. Opinion 4/2007 on the concept of personal data. WP 136. Brussels.

Article 29 Data Protection Working Party. 2012. Opinion 01/2012 on the data protection reform proposals. WP 191. Brussels.

Article 29 Data Protection Working Party, and Working Party on Police and Justice. 2009. The future of privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data. Brussels.

Barceló, Rosa, and Traung, Peter. 2010. The emerging European Union security breach legal framework: The 2002/58 ePrivacy Directive and beyond. In *Data Protection in a Profiled World,* eds. Serge Gutwirth, Yvers Poullet, and Paul De Hert, 77–104. Dordrecht: Springer.

Benoit-Rohmer, Florence. 2011. L'Union européenne et les droits fondamentaux depuis l'entrée en vigueur du Traité de Lisbonne. *Revue trimestrielle de Droit européen* 47 (1): 145–172.

Benyekhlef, Karim. 1996. Les normes internationales de protection des données personnelles et l'autoroute de l'information. In *Les Journées Maximilien-Caron: Le respect de la vie privée dans l'entreprise,* 65–101. Thémis.

Boehm, Franziska. 2012. *Information sharing and data protection in the Area of Freedom, Security and Justice*. Berlin: Springer.

Bougettaya, Farid. 2006. La protection des données personnelles en droit communautaire. Université de Montpellier I.

Burgorgue-Larsen, Laurence. 2005. Les juges face à la Charte: De la prudence à l'audace. In *La France face à la Charte des droits fondamentaux de l'Union européenne,* ed. Laurence Burgorgue-Larsen, 3–64. Bruxelles: Bruylant.

Bygrave, Lee A. 2010. Privacy and data protection in an international perspective. *Scandinavian Studies in Law* 56:165–200.

De Schutter, Olivier. 2005. Article II-68 - Protection des données à caractère personnel. In *Traité établissant une Constitution pour l'Europe: Commentaire article par article,* eds. Laurence Burgorgue-Larsen, Anne Levade and Fabrice Picod. Bruxelles: Bruylant, 122–152.

Docquir, Benjamin. 2009. Arrêt Satamedia: La (re)diffusion d'informations publiques dans les médias et les exigences de la protection des données. *Revue européenne de droit de la consommation* 2–3:560–581.

EU Agency for Fundamental Rights. 2012. Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package. FRA Opinion 2/2012. Vienna.

European Commission. 2000. File note: Comparative analysis of the Member States' legislation concerning the access to documents. SG.C.2/L D(99). Brussels.

European Commission. 2003. First report on the implementation of the Data Protection Directive (95/46/EC). COM (2003) 265 final. Brussels.

European Commission 2005. Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. COM (2005) 475 final. Brussels.

European Commission. 2007. Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM (2007) 87 Final, Brussels, 7.3. 2007, 8. COM (2007) 87 final. Brussels.

European Commission. 2009. Communication from the Commission to the European Parliament and the Council—Area of Freedom, Security and Justice serving the citizen. COM/2009/0262 final. Brussels.

European Commission. 2010a. Communication from the Commission to the European Parliament and the Council: Overview of Information Management in the Area of Freedom, Security and Justice. COM (2010) 385 final (2010). Brussels.

European Commission. 2010b. Communication from the Commission: Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union. COM (2010) 573. Brussels.

European Commission. 2010c. Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal Data Protection in the European Union. COM (2010) 609 final.

European Commission. 2012a. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM (2012) 11 final. Brussels.

European Commission. 2012b. Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. COM (2012) 10 final. Brussels.

European Commission. 2012c. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding privacy in a connected world: A European Data Protection framework for the 21st Century. COM (2012) 9 final. Brussels.

European, Data Protection Supervisor (EDPS). 2011. Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—'A Comprehensive Approach on Personal Data Protection in the European Union' *OJ C181/1*.

Gaeoudjiparl. 2012. *El camino del hardcore*. Barcelona: Alku.

Geyer, Florian. 2008. Taking stock: Databases and systems of information exchange in the Area of Freedom, Security and Justice. CEPS Research Paper No. 9. Centre for European Policy Studies (CEPS).

González Fuster, Gloria. 2012. Balancing intellectual property against data protection: A new right's wavering weight. *IDP Revista de Internet, Derecho y Política* 14:43–46.

González Fuster, Gloria. 2013. Security and the future of personal data protection in the European Union. *Security and Human Rights* 23 (4): 331–342.

González Fuster, Gloria, De Hert, Paul, Ellyne, Erika, and Gutwirth Serge. 2010. Huber, Marper and others: Throwing new light on the shadows of suspicion. INEX Policy Brief No. 11. Centre for European Policy Studies (CEPS).

González Fuster, Gloria, and Gellert, Raphaël. 2012. The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers & Technology* 26 (1): 73–82.

González Fuster, Gloria, and Gutwirth, Serge. 2013. Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review* 29:531–539.

González Fuster, Gloria, and Paepe, Pieter. 2008. Reflexive governance and the EU third pillar: Analysis of data protection and criminal law aspects. In *Security Versus Justice? Police and Judicial Cooperation in the European Union,* eds. Elspeth Guild and Florian Geyer. Aldershot: Ashgate.

González Vaqué, Luis. 2006. El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EE.UU. para la transmisión de datos sobre los pasajeros de las compañías aéreas. *Revista Española de Derecho Europeo* 20:557–576. (octubre-diciembre).

González Vaqué, Luis. 2008. El TJCE se pronuncia sobre la obligación de comunicar datos personales a fin de garantizar la protección de los derechos de autor en un procedimiento civil: La Sentencia 'Promusicae'. *Unión Europea Aranzadi* 5 (año XXXIV): 5–14.

González Vaqué, Luis. 2010. El TJUE precisa el alcance de la protección de los datos personales en el marco del acceso a los documentos de las instituciones de la UE: La Sentencia 'Comisión/Bavarian Lager'. *Gaceta Jurídica de la Unión Europea y de la Competencia* 18: 9–18. (noviembre-diciembre).

Groussot, Xavier. 2008. Case C-275/06, Productores de Música de España (Promusicae) V. Telefónica de España SAU, Judgment of the Court (Grand Chamber) of 28 January 2008: Rock the KaZaA: Another clash of fundamental rights. *Common Market Law Review* 45:1745–1766.

Guerrero Picó, María del Carmen. 2005. El derecho fundamental a La protección de datos de carácter personal en la Constitución Europea. *Revista de Derecho Constitucional Europeo* 2005 (4): 293–332.

Guichot, Emilio. 2008. Un paso decisivo en la clarificación de las relaciones entre derecho de acceso y derecho de protección de datos: La Sentencia del TPI de 8 de noviembre de 2007, Bavarian Lager/Comisión, T-194/04. *Revista Española de Derecho Europeo* 27:329–345. (julio-septiembre).

Guild, Elspeth, and Brouwer, Evelien. 2006. The political life of data: The ECJ decision on the PNR agreement between the EU and the US. Policy Brief No. 109. Centre for European Policy Studies (CEPS).

Gutwirth, Serge. 2007. Biometrics between opacity and transparency. *Annali dell'Istituto Superiore di Sanità* 43 (1): 61–65.

Gutwirth, Serge, and Hildebrandt, Mireille. 2010. Some caveats on profiling. In *Data Protection in a Profiled World,* eds. Serge Gutwirth, Yves Poullet, and Paul De Hert, 31–41. Springer.

Herlin-Karnell, Ester. 2009. Case C-301/06, Ireland V. Parliament and Council, Judgment of the Court (Grand Chamber) of 10 February 2009, Not yet reported. *Common Market Law Review* 46:1667–1684.

Hustinx, Peter J. 2005. Data protection in the European Union. *Privacy & Informatie* 2:62–65.

Jacqué, Jean-Paul. 2003. L'évolution des travaux de la Convention. In *Constitution européenne, démocratie et droits de l'homme,* eds. Gérard Cohen-Jonathan and Jacqueline Dutheil de la Rochère, 25–42. Bruxelles: Bruylant.

Korff, Douwe. 2004. The legal framework: An analysis of the 'Constitutional' European approach to issues of data protection and law enforcement. UK Information Commissioner Study Project: Privacy & Law Enforcement.

Kranenborg, Herke. 2008. Access to documents and data protection in the European Union: On the public nature of personal data. *Common Market Law Review* 45 (4): 1079–1114.

Le Bot, Olivier. 2003. Charte de l'Union européenne et Convention de sauvegarde des Droits de l'homme: La coexistence de deux catalogues de droits fondamentaux. *Revue trimestrielle de droit européen* 55:781–811.

Lind, Anna-Sara, and Magnus Strand. 2011. A new proportionality test for fundamental rights? The Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) V. Land Hessen. *European Policy Analysis* 7:1–12.

Mari, Gaia. 2008. Saggi—L'Unione Europea impone di non sacrificare ad occhi chiusi la proprietà intellettuale sull'altare della privacy. *Il Diritto di Autore* 3: 289–321.

Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.

Mayer-Schönberg, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton and Oxford: Princeton University Press.

Mendez, Mario. 2007. Passenger Name Record agreement: European Court of Justice. *European Constitutional Law Review* 3 (1): 127–147.

Murillo, de la Cueva, Lucas Pablo. 2009. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. In *El derecho a la autodeterminación informativa,* eds. Pablo Lucas Murillo de la Cueva and José Luis Piñar Mañas, 11–80. Madrid: Fundación Coloquio Jurídico Europeo.

Oliver, Peter. 2009. The protection of privacy in the economic sphere before the European Court of Justice. *Common Market Law Review* 46:1443–1483.

Pedilarco, Emanuele. 2006. Protezione dei dati personali: La Corte di Giustizia annulla l'accordo Unione Europea—Stati Uniti sul trasferimento dei dati dei passeggeri aeri. *Diritto Pubblico Comparato ed Europeo Vol. 3,* 1225–1231.

Pérez Asinari, María Verónica. 2004. La regulación de los datos de tráfico en la Unión Europea: ¿Entre la seguridad y los derechos fundamentales? *Lexis Nexis* II (4): 49–59.

Poullet, Yves. 2006. The Directive 95/46/EC: Ten years after. *Computer Law & Security Report* 22:206–217.

Poullet, Yves, and María Verónica Pérez Asinari. 2004. Données Des Voyageurs Aériens : Le Débat Europe-États Unis. Journal Des Tribunaux 12 (113): 266–274.

Quilleré-Majzoub, Fabienne. 2005. Les individus face aux systèmes d'information de l'Union européenne: L'impossible équation du contrôle juridictionnel et de la protection des données personnelles au niveau européen? *Journal du Droit International* 132 (3): 609–635.

Rallo Lombarte, Artemi. 2003. Europa ¿Hacia una Constitución europea? Reflexiones sobre la protección de los derechos fundamentales en el debate constituyente europeo. *Revista Valenciana de Economía y Hacienda* 7:201–218.

Rallo Lombarte, Artemi. 2010. El derecho al olvido y su protección: a partir de la protección de datos. *Telos: Cuadernos de Comunicación e Innovación* 85:104–108.

Reding, Viviane. 2012. The European data protection framework for the twenty-first century. *International Data Privacy Law* 2 (3): 119.

Rodotà, Stefano. 2009. Data protection as a fundamental right. In *Reinventing Data Protection?* eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 77–82. Dordrecht: Springer.

Rosen, Jeffrey. 2012. The right to be forgotten. *Stanford Law Review Online* 64 (2012) http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf. Accessed 10 March 2013.

Rosier, Karen. 2008. La Directive 2002/58/CE vie privée et communications électroniques et la Directive 95/46/CE relative au traitement des données à caractère personnel: Comment les (ré) concilier? In *Challenges of Privacy and Data Protection Law: Perspectives of European and North American Law,* eds. María Verónica Pérez Asinari and Pablo Palazzi, 328–352. Bruxelles: Bruylant.

Rouvroy, Antoinette, and Thomas Berns. 2010. Le nouveau pouvoir statistique ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps "numériques". *Multitudes* 40:88–103.

Soto García, Mercedes 2008. TJCE—Sentencia de 29.01.2008, Promusicae, C-275/06– Sociedad de la información, protección de datos personales, deber de divulgación de proveedores de servicios, protección de los derechos de auto. *Revista de Derecho Comunitario Europeo* 31:867–883.

Spiecker gen, Döhman, Indra, and Markus Eisenbarth. 2011. Kommt das 'Volkszählungsurteil' Nun durch den EuGH? – Der Europäische Datenschutz Nach Inkrafttreten des Vertrags von Lissabon. *Juristenzeitung* 4:169–177.

Terrasi, Alfredo. 2008. Trasmissione dei dati personali e tutela della riservatezza: L'accordo tra Unione Europea e Stati Uniti del 2007. *Rivista di Diritto Internazionale* 91:375–419.

Vranes, Erich. 2003. The final clauses of the Charter of Fundamental Rights—Stumbling blocks for the first and second Convention. European Integration online Papers (EIoP) Vol. 7 No. 7.

Chapter 8
Conclusions

> *Le traducteur est un écrivain d'une singulière originalité, précisément là où il paraît n'en revendiquer aucune. Il est le maître secret de la différence des langues, non pas pour l'abolir, mais pour l'utiliser, afin d'éveiller, dans la sienne, par les changements violents ou subtils qu'il lui apporte, une présence de ce qu'il y a de différent, originellement, dans l'original.('The translator is a writer of singular originality, precisely where he seems to claim none. He is the secret master of the difference of languages, not in order to abolish the difference but in order to use it to awaken in his own language, through the violent or subtle changes he brings to it, a presence of what is different, originally, in the original' (translation by Elizabeth Rottenberg))*
>
> (Blanchot 1971, 1997)

This inquiry into the emergence of the EU fundamental right to the protection of personal data allows to draw a series of important conclusions on the way in which such emergence has occurred, or the question of *how* could this new right surface in EU law. But it can also help to obtain an enhanced understanding on the right's nature and status, or the question of *what* has emerged. The main point of this book is precisely that, in order to fully understand the significance of this emerging EU fundamental right, it is necessary to take into account the complex interplay between the different legal notions that led to the right's birth, because this interplay still affects its evolution.

Obtaining a refined understanding of the EU fundamental right to personal data protection appears to be particularly timely. The EU legislator is nowadays addressing a long-awaited review of the European data protection legal framework, and the new right is foreseeably to play a protagonist role in any upcoming legal instruments. Despite the increasing prominence of the new right, however, the doctrine is unfortunately still struggling to delimit the new reality (Purtova 2010, p. 182; Tzanou 2013, p. 99). This chapter will not only be useful to improve the understanding of the EU right to personal data protection, but can also help to comprehend some of the reasons behind such lingering struggle.

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_8,

8.1 How Did the EU Fundamental Right to Personal Data Protection Emerge

The complex interplay between legal notions leading to the surfacing in EU law of the fundamental right to the protection of personal data is best described as a series of legal operations of distinction and in-distinction. This means that notions such as 'privacy', 'private life', 'data protection' and 'personal data protection' have over the years sometimes functioned in EU law as distinct, different, and separate, whereas in some occasions they have worked as equal or at least equivalent, or in-differentiated (thus, not as the object of any distinction). These operations of distinction and in-distinction taking place through the occurrences of law have affected the very meaning of the legal words involved:[1] in this sense, they have been productive, giving way to the unfolding of new legal objects rendering possible further new operations of distinction and in-distinction.

8.1.1 A Process of Legal Miscommunication

Some of the identified operations can be viewed as embedding in law crucial (mis)translations. For instance:

- the naming of any European national laws on the processing of data about individuals as 'data protection' laws, formalised in 1981 as the Council of Europe completed its Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data ('Convention 108') took place despite the fact that none of the existing European laws to which this instrument referred to had been previously labelled as 'data protection' laws.[2] Thus, Convention 108 not only created a new label ('data protection'), but also established that this new notion was at least roughly equivalent to legal notions previously developed at national level;
- likewise, the naming of any national laws on the processing of data about individuals as 'privacy' laws, embodied by the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 by the Organisation for Economic Co-operation and Development (OECD), under direct United States (US) influence, took place even though none of the existing European laws to which the Guidelines referred had been previously labelled as 'privacy' laws. As a result of the coexistence of Convention 108 and the OECD Guidelines, national rules on data processing became classifiable not just as 'data protection' laws but also as 'privacy' laws, depending of the adopted perspective.

[1] Just as translations have the power to alter the meaning of the original text (Benjamin 1992, p. 73).

[2] German laws took the name of *Datenschutz*, an expression from which was derived the English 'data protection', but that had a specific meaning, referring only to data automatically processed.

This, in its turn, sustained the semblance of an equivalence between the notions of 'data protection' and 'privacy';

- the designation of the right to respect for private life of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) as a right to 'privacy', initiated in the context of the Council of Europe at the end of the 1960s under indirect US influence, reproduced by Convention 108 in 1981, and reverberated in Directive 95/46/EC (marking its formal incorporation into EU law), in a sense misread Article 8 of the ECHR, which does not refer to any privacy but to a right to respect for private life: confirming that Article 8 of the ECHR is concerned with the right to respect for private life, and not with 'privacy', the European Court of Human Rights (ECtHR), despite having ostensibly expanded the interpretation of Article 8 of the ECHR as to cover some aspects of data protection in the sense of Convention 108, and even if it has repeatedly used the words 'data protection', has persistently refused to openly embrace the term 'privacy' to allude to the content of Article 8 of the ECHR;
- the identification of the insurance of the right to privacy (in the sense of Article 8 of the ECHR) as the prime purpose of 'data protection' laws, as per Convention 108 and Directive 95/46/EC, neglected the fact that existing national rules on data processing had hardly ever been explicitly designed to pursue such target. In reality, the approach encapsulated by Convention 108 and Directive 95/46/EC, according to which 'data protection' laws primarily serve 'privacy' (or the respect for private life), was alien to the majority of early European legislation on data processing. In this sense, it was extraneous, for instance, to seminal German *Datenschutz* instruments. In 1976, Portugal had inserted into its Constitution a provision on the automated processing of data, unattached to any reference to privacy, or private life. In 1978, France had adopted a law on 'computers and freedom' (*informatique et libertés*), connecting it to the notion of *vie privée* (which, in accordance with the Universal Declaration of Human Rights, could indeed actually be regarded as equivalent to privacy), but attaching it also to the protection of human identity and, generally, of human rights, as well as of individual and public freedoms. And, also in 1978, Austria had granted constitutional-level protection to a right to *Datenschutz* ('data protection'), defined in terms that connected such right to a safeguarding of the 'private life' of individuals, but this Austrian right was a right nonetheless recognised as a right per se;[3] and

[3] When Member States had to transpose Directive 95/46/EC, the diversity of national approaches towards the fundamental rights framing of personal data protection norms became particularly visible: whereas some, such as Belgium, already mirrored in their legislation the idea according to which the regulation of personal data primarily pursues the protection of privacy (*persoonlijke levensfeer/vie privée*), others appeared to lack a legal notion perceived as fully corresponding to the 'privacy' targeted by EU legislation, as illustrated by the fact that some countries wrote new words into their legal systems (for instance, Spain, where a 1992 norm inspired by initial drafts of the Directive alluded to *privacidad*). In Italy, the implementing law disregarded the expression that the Italian version of Directive 95/46/EC had put forward as equivalent to privacy (*vita privata*), and replaced it with explicit references to dignity, *riservatezza* and personal identity, facilitating by the same token the recognition of these notions as constitutionally protected rights in Italy. Coinciding with this movement, Italian literature imported the word privacy to refer generally to

- the advancing in Article 8 of the EU Charter of a right to personal data protection as if corresponding to the rules on data protection established by Convention 108, or by Directive 95/46/EC, disregarded that Article 8 of the Charter's wording is not fully equivalent to Convention 108 or to Directive 95/46/EC; it operated as if 'personal data protection' (which is what the right of Article 8 of the Charter is about) was the same as 'data protection' (which is the subject of Convention 108 and Directive 95/46/EC), which is however presumably not the case, as the latter instruments describe their own purpose as, primarily, to ensure privacy, whereas Article 8 of the Charter is precisely presented as something different from privacy (or the right to respect for private life of Article 8 of the ECHR, to which is devoted Article 7 of the Charter).

The described events can be regarded as translations insofar as they pretend to mirror or reproduce in specific legal systems, and in specific legal instruments, notions present elsewhere. But they are also *mis*translations or *mis*interpretations to the extent that, in mirroring or reproducing some notions, they do not merely mimic or repeat existing meanings, but alter them. The *mis*readings of previously existing legal norms have resulted in new occurrences of law that generated displacements of meaning. These operations notably contributed to sustain a semblance of equivalence between the legal notions at stake. For instance, the naming of any European national laws on the processing of data about individuals as 'data protection' laws supported the possibility of them being alike, and their naming as 'privacy' laws sustained their envisioning as, if not identical, at least very similar to US privacy laws.

All in all, these developments show that the emergence of the EU fundamental right to personal data protection has at least partly pivoted on a complex relationship with the term privacy, which in its turn has also been affected by these operations.

Traditionally regarded as elusive and multifaceted, the word 'privacy' suffered a number of significant re-configurations since the 1960s, resulting in the further adscription to the term of new layers of meaning, notably associating it with computerised data processing, and with the notion of 'fair information practices'. It was with these particular layers of meaning that the word 'privacy' infiltrated Council of Europe's institutions at the end of the 1960s, in the context of discussions on the impact of technology upon human rights. The word thus brought in with it traces of a conceptual linkage with automated data processing, and with the American post-Westin conceptualisation of privacy as control upon personal information. As a consequence of the cumulative effect of the OECD Guidelines and Convention 108, privacy acquired two new major acceptations with regards to personal data protection: it could either refer to norms regulating the processing of personal data, or to the norms' main purpose. This duality firmly inscribed in the very word privacy a structural ambiguity (Pino 2006, p. 140), which concomitantly conditioned the

personal data protection laws. Many of the countries that were to become EU Member States in 2004 were also by then giving shape to their own laws on the protection of personal data, and in some cases to constitutional provisions overtly identifying a fundamental right to personal data protection, unconnected to any right to privacy.

understanding of Convention 108's notion of 'data protection': data protection became conceivable both *as privacy*, or, alternatively, as something *the main purpose of which is* (the human right to) *privacy*. Already in the 1970s, some continental languages such as Dutch had started to adopt the word privacy as their own, and their usage of the term typically mirrored this ambivalence, as well as the fluctuant privacy/data protection nexus.

This structural ambiguity of the word privacy is indeed not confined to its appearances in English. Crucially it also affects the meaning of the non-English words that are recognised as equivalent to it by EU law. The coexistence of multiple linguistic versions of legal instruments as authentic versions entrenches in EU law the (at least) partial equivalence between words of different languages. Based on the mere reading of Directive 95/46/EC, the English privacy has to be regarded as equivalent to (in the sense of mutually translatable with) the Dutch *persoonlijke levenssfeer*, the French *vie privée*, the German *der Privatsphäre*, the Spanish *intimidad*, the Italian *vita privata*, the Portuguese *vida privada*, or the Swedish *privatliv*. Read together with Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector,[4] privacy surfaces additionally as (sometimes) interchangeable with the Dutch *privacy*, the German *Datenschutz*, the Spanish *privacidad*, the Portuguese *privacidade*, or the Swedish *integritet*. These are to be regarded not only as acceptable translations, but actually as equally authentic words with equivalent meaning (for the purposes of EU law).

From this standpoint, it appears that the evolution of personal data protection in Europe can not only be understood as linked to processes of international communication,[5] but also conceived as deeply indebted to processes of legally upheld miscommunication.

8.1.2 Distinctions and In-distinctions

The emergence of the EU fundamental right to personal data protection has thus developed through a partial interchangeability in EU law of some legal terms, which it has also nurtured. This interchangeability has been crucial to enable EU law to shift from the absence of a right to its presence, constraining novelty and sustaining continuity. In this sense, the word 'privacy' is sometimes used as equivalent to 'respect for private life', as in Directive 95/46/EC, but it is also sometimes read as referring to data protection (laws), be it in line with the OECD Guidelines, for which any laws on the processing of information about individuals *are* privacy laws, or from the perspective of Convention 108 and Directive 95/46/EC, for which any laws on

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

[5] For a consideration of this approach and the evolution of international privacy, see notably: (Bennett 1997).

the processing of information about individuals *serve primarily* privacy (even if not only privacy), which makes them also somehow *privacy* laws. But, at the same time, the word 'privacy' can also be apprehended as referring to something different from (personal) data protection, in particular on the basis of Article 8 of the EU Charter.

Similarly, the phrases 'data protection' and 'personal data protection' are sometimes used in English as referring to an identical legal notion, as if the later was a short denomination of the former; but they can also be envisioned as different legal notions: Convention 108 is overtly concerned with what it calls 'data protection' (that it defines as the respect, with regard the automatic processing of personal data, of the rights and fundamental freedoms of individuals, and in particular of their right to privacy), whereas Article 8 of the EU Charter is formally devoted to a right to 'personal data protection', advanced as something different from the right to respect for private life/privacy.

It is on these ambiguities that the EU fundamental right to the protection of personal data has been built. Legal change has a discernible linguistic dimension: law evolves through the fluctuation of meaning between words. More precisely, in order to evolve, law relies on words capable of both denoting their belonging to the legal system (Luhmann 2012, p. 20), and being read, in due time, with an unprecedented meaning. Change in reading and re-writing is enabled by the vocabulary of law, but also by other linguistic features such as specific co-occurrences of words, and substitutions, which give means to the possibility of unstable readings. In a sense, law changes because it eventually mis-reads law, and because it always writes itself in a way triggering the possibility of further mis-readings.[6]

The multiplicity of languages operating in EU law is a privileged locus for the transfers of meaning underpinning legal change. Just as any translation must imperatively accept a degree of departure from the original, different linguistic versions of a same legal text obligatory encompass gaps, or fractures between versions, which EU law nonetheless blocks out through the fiction of equivalence. The fictional equivalence of EU official languages asserts equivalences between words that can necessarily only be partial, and thus inscribes in words an ambivalence[7] upon which can take effect legal operations of (in)distinction.

The emergence of the EU right to personal data protection can thus be located in a series of legal operations of coupling and un-coupling between 'privacy' and (personal) data protection, at the heart of which lies the described partial interchangeability of these words, which is inseparable from the (*mis*)translation events identified above.

Operations of coupling can take many forms. Some have already been highlighted: privacy and data protection were famously connected in Convention 108 (with the formula 'data protection serves (primarily) privacy'), but also implicitly by the OECD Guidelines, an instrument that regards as comparable any laws

[6] And thus constantly sustain the interplay of traces inscribed in words (Kruger 2004, p. 57).

[7] On ambiguity as a requirement of 'mediators' ensuring the coherence of translation networks, see: (Callon 2006, p. 249).

regulating the processing of information about individuals (and thus include European 'data protection' instruments under the privacy tag). The renaming of the right to respect for private life of Article 8 of ECHR as a right to privacy, together with the partial integration of the substance of Convention 108 under its scope by the case law of the ECtHR, indirectly lead to the setting up 'data protection' as an element of that 'right to privacy'. This idea was further reinforced by Directive 95/46/EC and, even strongly, by the EU Court of Justice's early reading of Directive 95/46/EC.

The EU Court of Justice had indeed ruled that, in order to apply EU personal data protection laws, it must always be remembered that they serve the right to privacy, and, thus, what must be applied is (directly, simply, exclusively) the right to respect for private life of Article 8 of the ECHR.[8] From this perspective, the Luxembourg Court has occasionally not recognised any relevant difference between EU personal data protection and the right to respect for private life — in what can be described as operations of coupling of legal notions, or of legal in-distinction.[9]

In the case law of the EU Court of Justice, the in-distinction of data protection and privacy has produced (and has been punctually preserved by) explicit affirmations of the close relationship linking personal data protection and privacy. Their conceptualisation attained a yet unsurpassed level of absence of differentiation with the finding by the EU Court of Justice of a single *right to respect for private life with regard to the processing of personal data*, recognised jointly by Articles 7 and 8 of the Charter, in the *Schecke and Eifert* judgment.[10] This almost incessant latent in-distinction reduced the potentially disruptive impact of EU Charter's assertion of a right to personal data protection. But it does not prevent the possible acknowledgement of a distinction between the content of Article 8 of the Charter and the right to respect for private life, also potentially sustained by the Charter.

Data protection and privacy have also been coupled through diverse combined occurrences in EU secondary law. After the solemn proclamation of the EU Charter of Fundamental Rights in 2000, and until the entry into force of the Lisbon Treaty in 2009, EU secondary law witnessed the proliferation of joint references to data protection and privacy, put forward together as seemingly undifferentiated, or as attached by an unspecified relatedness.

The incorporation in the EU Charter of a provision on personal data protection (in its Article 8) separated from the provision devoted to the right to respect for private life (in Article 7) facilitated the legal un-coupling of the two notions. The Charter, however, also allows the reading of the two as indistinguishable. Such potential lack of distinction is sustained both through the Charter's Article 7 and 8. First, by the formal correspondence between Article 7 of the Charter and Article 8 of the ECHR, a provision which, according to established ECtHR case law, encompasses

[8] Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, Judgment of the Court of 20 May 2003.

[9] Coupling produces difference through indifference (Luhmann 2012, p. 107).

[10] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, Judgment of the Court (Grand Chamber) of 9 November 2010 § 52.

some features related to the protection of individuals against the processing of information about them, thus potentially matching safeguards covered by Article 8 of the Charter. This can be interpreted as an invitation to read data protection as an element of privacy, even in the Charter's context. Second, a plausible inseparability or indistinguishableness between personal data protection and respect for private life is also upheld by the connections instituted between Article 8 of the Charter and a series of other legal instruments, on which the provision is allegedly based, and that attach the protection of personal data to fundamental rights and freedoms in general, but specifically to the right to privacy (to be understood here as respect for private life) of Article 8 of the ECHR. In this sense, the Explanations accompanying the Charter, now officially legally relevant for its interpretation, indeed condition the expounding of Article 8 of the Charter to instruments such as Convention 108 and Directive 95/46/EC, which explicitly link the protection of personal data to the right to privacy.

Nevertheless, there have been in EU law already a number of operations of uncoupling between (personal) data protection and privacy. An instance of a significant legal distinction between privacy and data protection surfaced in EU law in the context of exceptions to the right to access to documents; concretely, the exceptional refusal of access foreseen by EU law for cases where what is at stake is privacy 'in particular in accordance with' EU personal data protection provisions. In its judgment on this issue, the EU Court of Justice decided that to apply privacy 'in accordance with' personal data protection must mean something different than to merely apply privacy; therefore, it granted legal significance to the distinction between just privacy and privacy together with personal data protection.[11] Facilitating this explicit recognition of a difference between privacy and personal data protection, the term 'privacy' had surfaced in this specific context (that is, the area of access to documents) through a peculiar genealogy. It was not rooted in Directive 95/46/EC, or in Convention 108, but in traditional national exceptions to access to documents. It was thus less marked by the coupling of data protection and privacy sustained by Convention 108 and Directive 95/46/EC.

The possibility for courts to sometimes sustain a distinction, and sometimes disregard it, is entrenched in the words that law uses. The meaning of these words is always conditioned by other legal occurrences; hence, by the passing of time, and by the temporal unfolding of case law and legal provisions.

8.1.3 An Emergence to Come

Article 8 of the Charter marked a key step in the emergence of the right to personal data protection in EU law, but cannot be regarded as amounting by itself to the culmination of a process of recognition, or of integration into EU law. Such a process

[11] See C-28/08 P *Commission v Bavarian Lager* [2010] ECR I-6055, Judgment of the Court (Grand Chamber) of 29 June 2010.

is as a matter of fact still on-going, and its outcome is dependent on the constant reading and re-writing of Article 8 of the Charter both in EU positive law, and in the EU Court of Justice's case law.

Although historically some backed up the elaboration of a written catalogue of EU rights as a step towards legal certainty, to write law is not to settle law. The validation by the Charter of a possible distinction between the rights of Articles 7 and 8 opens up, in its turn, multiple avenues for further oscillations in the construal of these identifiable rights. It notably raises the question of the possible correspondence of the right established by Article 8 of the Charter with the object of Convention 108 and of Directive 95/46/EC, on which it is based, and which are instruments concerned (overtly or implicitly, respectively) with 'data protection'. As noted, in English the expression 'data protection' can as a matter of fact be read both as a notion per se (and it is as such, formally, the object of Convention 108), or as an elliptical construction—a short name for 'the protection of personal data', or 'personal data protection', which is the distinct denomination of Article 8 of the Charter. This ambivalence of the English 'data protection' allows using this phrase to allude to both realities. This duality, however, does not exist in other European languages, that mark formally a difference between 'data protection' and 'personal data protection': for instance, in German (*Datenschutz* vs. *Schutz personenbezogener Daten*), or in Swedish (*dataskydd* vs. *skydd av personuppgifter*). In these languages, in 'data protection' are seemingly still too visible the traces of a legal notion that personal data protection as per Article 8 of the Charter might transcend (or not, depending on whether law further builds on this distinction).

As this reading and re-writing unfolds, a new possible oscillation in the Charter's interpretation has become manifest, as a reminder of the permanent undecidability of law. This oscillation concerns the possibility of envisioning the EU right to personal data protection either as established by the Charter's Article 8 as a whole, or solely by its first paragraph.[12] In the first case, the right to personal data protection is understood as comprising the six basic constituents described in its second and third paragraphs: the requirement of fair processing; the requirement of processing for specified purposes; the requirement of legitimate basis (a basis laid down by law, or the consent of the person concerned); a right of access to data; a right to have data rectified; and independent supervision. In the second case, the right is conceived of as being set out in the Charter's Article 8(1) (reading 'Everyone has the right to the protection of personal data concerning him or her'), whereas Articles 8(2) and 8(3) would describe requirements for the right's limitations to be lawful, applicable whenever personal data are processed. This reading implies that to have personal data protected would mean, in principle, to have personal data un-processed.

These oscillations in reading can thus affect the meaning of the notion 'personal data protection', and, more concretely, the understanding of the essence of such 'protection'. From the first perspective, 'personal data protection' would contain as core constituents the mentioned requirements applying not only to the data as

[12] For instance, see: C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* [2011] ECR I-3441, Judgment of the Court (Third Chamber) of 5 May 2011 § 49.

such, but also to those who process it, and to those to whom it relates, as well as a requirement of control by a supervisory authority. From the second viewpoint, conversely, the right to 'personal data protection' would merely imply that personal data must be protected in the sense of left un-processed, untouched, safeguarded (unless in compliance with Article 8(2) and 8(3) of the Charter): it would be a sort of right for data to be 'let alone'. This latter view might superficially appear to be sound, as, taken in isolation, the expression 'personal data protection' can seem to allude to the protection *of personal data*. This idiom was however already recognised as a misnomer when it surfaced as *Datenschutz* in the 1970 *Datenschutzgesetz* of the federal state of Hesse (Burkert 1999, p. 46): it could came across as being concerned with a sheltering *of data*, but legally it encompassed much more. Understood not in isolation, but in the light of Convention 108 and of Directive 95/46/EC, 'data protection' is certainly something different from a mere prohibition to process personal data.[13]

Until now, the EU Court of Justice has only occasionally ventured to adjudicate on the basis of Article 8 of the Charter without linking its interpretation to Article 8 of the ECHR,[14] and it has not yet decisively clarified whether it regards the right to personal data protection to be infringed as soon as personal data are processed,[15] or only when data are processed without full compliance with Articles 8(2) and 3 of the Charter. The judiciary rules, determines, decides, but it never entirely resolves law's open-texture (Alexy 2010, p. 3).

8.1.4 Implications on the Understanding of the Origins of the Right

In the emergence of the right to personal data protection, the word privacy appears as central conveyor of ambivalence. Present in all existing major international and European legal instruments related to the processing of personal data, the word privacy has sustained both recursivity and variation in these norms. Possibly absent from the future EU personal data protection legal landscape, it will certainly nevertheless, despite its foreseeable spectral status, continue to influence the further reading and re-writing of EU personal data protection laws. The historical centrality of the word 'privacy', nonetheless, should not be interpreted as implying that the

[13] Against the characterisation of personal data protection as prohibitive: (Gutwirth 2007, p. 63) (cf. however with the observation that 'at first glance' Directive 95/46/EC 'seems to create a system of general prohibition' by establishing requirements for the legitimacy of data processing in (Gutwirth and De Hert 2008, p. 282)).

[14] Notably in C-70/10 *Scarlet Extended SA* v *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgment of the Court (Third Chamber) of 24 November 2011, not yet published; and C360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, Judgment of the Court (Third Chamber) of 16 February 2012, not yet published.

[15] See, precisely, *Scarlet* and *Netlog*.

surfacing of personal data protection has been exclusively authored by a specific notion, a particular approach, or a single word. It is the interplay between different legal occurrences, including different legal occurrences in different languages, which generated and allowed for such surfacing.

The roots of the legal notion of personal data protection are in a way not traceable back to any particular language, but rather to the interactions between different languages. These roots can be described as intertwined with the notion of privacy, as long as it acknowledged that the meaning of this word has been affected by the very materialisation of personal data protection. Data protection was built up as potentially conceivable *as privacy*, and thus privacy sometimes appeared to be conceivable *as data protection*. In this reciprocal construction came to be also involved the right to respect for private life. The amalgamation of the English privacy and respect for private life was to some extent provoked, and certainly sustained, by their alternate use as synonymous to the French *vie privée* in international instruments, including data protection instruments.

The displacements of meaning through law encountered in our inquiry confirm that the languages of European law cannot be regarded as fully separate entities. The English 'data protection' might have originally surfaced as a borrowing from the German *Datenschutz*, but through its use in EU law it acquired new meanings, which eventually also affected the meaning of the German *Datenschutz*. The German word as nowadays used thus shows signs of being what linguists envision as round-trip loans or r-emigrant words (Gómez Capuz 2005, p. 60): taken from a language to another, and later reintroduced into the first with slight changes of signification. These round-trip loans are paradigmatic examples of the permeability of languages, and raise particularly arduous challenges when they need to be translated.[16]

The acknowledgement of these hybrid origins of the words used by EU law, inescapably engaging in intricate and reciprocal relationships, should not be understood as implying that EU law ensures the equal treatment of all the languages involved. In these transfers of meaning, some words, such as privacy, have actually acquired a dominant role. This prevalence could be described as a phenomenon of hegemony manifesting in a word, an English word, whose floating usage nonetheless invites to question to which languages it belongs (Derrida 2004, p. 565).

8.2 The Emerging EU Fundamental Right to Personal Data Protection

The legal operations allowing for the emergence of the EU fundamental right to personal data protection have generated displacements of legal meaning which have not been neutral, or without consequence. They have critically involved two significant transformations. First, the passage from a number of legal notions formally concerned with the regulation of a technological development (more specifically,

[16] See, for instance: (Wecksteen 2009, p. 137).

with the advent of computers) towards a right that is formally un-concerned with any specific technology. Second, the depiction of this new right as a 'EU fundamental right', a label built in parallel to the surfacing of EU personal data protection, and advanced by EU law as conventionally akin to national fundamental rights, as well as to international human rights.

8.2.1 Technology and the EU Right to Personal Data Protection

Multiple developments related to the emergence of European personal data protection are overtly concerned with technology, and, more particularly, computer technology. In Article 8 of the EU Charter, however, there is no reference to computers, or even to the automated processing of data. Its object is the processing of personal data, a legal category operating irrespective of the way in which data are processed. This in a way signals the culmination of a process of transformation, from a series of rules specifically devoted to the automated processing of data by computers towards a legal notion that is detached from them.

Technology matters. It certainly does. It has repeatedly been evoked in debates surrounding the formation of legal notions to which is connected the emergence of personal data protection in Europe, and it has influenced them.[17] The advent of computerisation, and particularly the computerisation of public administrations since the end of the 1960s, configured a context to which laws on the processing of personal data could be related, even if these laws could also have in principle be related to previous technological developments,[18] and de facto have been connected since to a myriad of other technological changes.

Technology, in any case, can also be concealed, dismissed, obliterated by law. The expression 'data protection' had been borrowed from the German *Datenschutz*, where *Daten* specifically denoted data undergoing automated processing, as opposed to any type of information. This specific layer of meaning was lost in translation already with the adoption of Convention 108, as, in English, 'data protection' (and, in French, *protection des données*) could potentially refer to any kind of information—even if, for the concrete purposes of Convention 108, as set out by its provisions, 'data protection' indeed applied solely to the automated processing of information (more precisely, to the automated processing of information qualifying as 'personal', in the sense of relating to an identified or identifiable individual). The transfer of *Datenschutz* into English (and French) in Convention 108 subtly made the traces of automated processing present in *Daten* legally irrelevant. When EU law took the idiom 'data protection' from Convention 108, it was thus able to expand its scope beyond the automated processing of personal data, to encompass

[17] Even a conception of law as 'social system', which emphasises its autonomy, recognises that no system is autarchic (even if its environment can only be integrated into the system by the system's communication synthesis) (see, in this sense: (Luhmann 1995, p. 144).

[18] One can think, for instance, of the invention of tabulated punch cards, and their use in Nazi Germany (on this subject, see for instance: (Luebke and Milton 1994)).

any processing of personal data. Directive 95/46/EC is formally concerned with the protection of individuals with regard to any processing of personal data. The Directive applies not exclusively to data undergoing automated processing, but also to data manually processed, and hence confirms that the term 'data' in the expression 'data protection' as endorsed by EU law shall not be read (anymore) as the German *Daten* in the original German *Datenschutz* provisions.

Technology alone does not suffice to explain legal change. The words of law decide to what extent technology matters for law, and how. This is why it is not only relevant, but also important to interrogate the evolution of law apprehended as text. Sometimes, law has dissolved the relevance of technological difference not in the vocabulary itself, but by dismissing the legal significance of a particular distinction (for instance, the distinction *computerised* vs. *manual processing*) and by asserting instead the relevance of another distinction (such as *personal data* vs. *no personal data*). This occurred in the re-writing of Article 18(14) of the Spanish Constitution performed by the Spanish Constitutional Court, which transformed a mandate to legislate *on computers* into a right to the protection *of personal data*. Likewise, the relevance of a distinction enabled by a legal provision can be discontinued merely because another provision sets out that this should be so; in this sense, Article 35 of the Portuguese Constitution, on the use of computers, now applies mutatis mutandis also when computers are not used, as established by its last paragraph.

8.2.2 Turning (Personal) Data Protection into a EU Fundamental Right

Personal data protection acquired the legal status of EU fundamental right through its coupling with, and eventual de-coupling from, privacy, understood as a right enshrined by Article 8 of the ECHR. Originally, EU data protection laws enjoyed a 'human rights' dimension because of their connection to the ECHR. In due course, this particular attachment allowed for EU personal data protection to acquire in its turn a status of 'fundamental right', the legal significance of which is affected by the progressive dethroning of privacy as the key right for the interpretation of EU data protection law.

To apprehend how words engage in law's change, it is necessary to take into account not only the words appearing in the occurrences of law, but also those that disappear—and how they do it. Absence transfers meaning (Luhmann 2012, p. 20). The settlement of the fundamental right to personal data protection in EU law entered a new phase as the EU Court of Justice started to stop ostensibly basing the right's reading upon Article 8 of the ECHR, and a new twist has been heralded by the legislative package on the protection of personal data put forward by the European Commission in January 2012.

This legislative package announces the disappearance of the word privacy, and of references to Article 8 of the ECHR, from the main instruments of EU personal data protection law. In the proposals submitted by the European Commission, the

right to protection of personal data has supplanted the right to privacy. It takes its role, replacing it in Convention 108's formula *data protection serves in particular privacy*: the formula's template has been maintained, but its content has been transformed. Its new form is *(personal) data protection serves in particular the (EU right to) the protection of personal data*. This move posits the equivalence, or at least *an* equivalence, between the emergent right to personal data protection and the established right to privacy/respect for private life. They are here envisaged as distinct, but comparable. Different, but matching each other. And what this substitution ultimately predicates is that it is possible to replace a right recognised as a human right in the ECHR with a right established, as a EU fundamental right, in the Charter, as well as that the latter deserves protection by itself.[19]

To some extent, at least, the right to personal data protection is a EU finding, as opposed to a creation of Member States, or of the Council of Europe. It has surfaced as such at the margins of EU's insurance of fundamental rights as 'general principles' of EU law, 'general principles' which are determined on the basis of the common constitutional traditions of Member States, and of the ECHR. The right to the protection of personal data cannot be derived (or at least, not derived in its entirety, and as a right per se) from any of the sources that ground EU's architecture for the protection of fundamental rights. Its integration into this architecture is thus a crucial element of its emergence as EU fundamental right.

Arguably, the EU legislator has since the Lisbon Treaty no other choice than to legislate in the field of personal data protection on the basis of Article 16 of the Treaty of the Functioning of the EU, and thus it must, imperatively, frame upcoming instruments in the area under the emerging EU fundamental right to personal data protection. It has the choice, however, to accompany or not any invocation of the right to personal data protection with a reference to Article 7 of the Charter, or to Article 8 of the ECHR, on the right to respect for private life. By avoiding the until now conventional (re)statement of such linkages, the European Commission's 2012 legislative proposal is amplifying the now intermittently acknowledged distinction between Article 7 and Article 8 of the Charter, but reproducing it in a new form, that could have a definitive impact on the right's emergence as a fundamental right.

8.2.3 The Meaning of Fundamental

If integrated into a Regulation, the EU fundamental right to personal data protection would directly enter into EU national legal systems, some of which have already their own fundamental rights to the protection of personal data, or similar constitutionally protected rights, or, still, a constitutional mandate to legislate in the field under certain particular conditions. Whereas Directive 95/46/EC left the door open for Member States to freely convert the instrument's fundamental rights framing into their own national context, a Regulation would straightforwardly connect its

[19] Describing this as problematic (in relation with the distinction by the Charter between the right to respect for private life and personal data protection): (Rouvroy and Poullet 2009, p. 74).

provisions to the new EU fundamental right, which actually does not exactly correspond to any national fundamental right.

The proposed Regulation has already generated criticism in Germany precisely on the grounds of its (exclusive) ties with Article 8 of the EU Charter, judged potentially contrary to the German system of fundamental rights protection, and possibly unlawfully undermining the competences of the German Federal Constitutional Court.[20] To the extent that the EU fundamental right to personal data protection overlaps with national fundamental rights, its legislative development by the means of a EU Regulation inevitably generates frictions with requirements derived from national fundamental rights. A solution to this problem might reside in the open recognition of the distinction between national fundamental rights, on the one hand, and EU fundamental rights, on the other. The ambiguity between these two notions, however, has been traditionally strongly backed up by the EU to uphold its own legitimacy: by claiming that it safeguarded EU fundamental rights, EU law portrayed itself as unable to infringe national fundamental rights. Now, paradoxically, this ambiguity might generate new problems.

What is questionable in any case is the substantial equivalence between national and EU fundamental rights seemingly predicated by the move described above. The emergence of the right to the protection of personal data as a EU fundamental right is also the fabrication of a new type of 'fundamental' right, through a variation of the meaning of the adjective 'fundamental'.

The 'fundamental' nature formally attributed by the Charter to the right to the protection of personal data is based on an act of naming of the Charter itself. It does not correspond to any specific definition of fundamental right. The Charter, despite having the same legal value as EU Treaties, de facto conditions the interpretation of the right to the protection of personal data to the content of its accompanying Explanations, which in their turn refer to EU secondary law instruments echoing both considerations related to human rights (in particular, the right to privacy) and single market priorities, such as the free flow of personal data. This notion of free flow is additionally explicitly enshrined in the Treaties themselves, which the EU Charter also regards as relevant for the interpretation of its own provisions, including of its Article 8. In reality, nowadays the free flow of data, originally imported into EU law by Directive 95/46/EC,[21] is not only recognised as such by the Treaties, but has been extended beyond the single market to the whole spectrum of activities falling under EU law, including the Area of Freedom, Security and Justice (AFSJ).

[20] In this sense: (Hornung 2012).

[21] Directive 95/46/EC transferred into EU law from Convention 108 (and thus, indirectly from the OECD Guidelines) the notion of the 'free flow' of information, in terms of a free flow of personal data, and assigned it to the establishment of the single market. By doing so, it positioned this free movement of personal data as one of the 'fundamental (market) freedoms' recognised by EU law, together with other freedoms such as the free movement of people, goods, services and capital. The EU Court of Justice has construed these fundamental freedoms as not only essential, but foundational, in the sense that they touch upon the very foundations of the EU. The Luxembourg Court has conceded, nonetheless, that in some circumstances these fundamental freedoms can conflict with fundamental rights; in such cases, states the Court, a balance between them shall be struck.

Thus, the Charter of Fundamental Rights of the EU, in spite of its emphatic name, solemn proclamation and Treaty-like legal value, enshrines a 'fundamental' right bearing inside it a balancing between human rights considerations and (extended) free market priorities: a right to personal data protection that must imperatively be interpreted in the light of, and balanced with, the comprehensive free flow of personal data.

8.3 Disentangling Privacy and Personal Data Protection?

To envisage law as continuously renegotiating the meaning of the words of law obliges to refrain from any determination of the content of legal notions that would be valid in abstract, and to accept meaning as in a constant state of flux. It cannot be concluded from the evidence gathered, thus, whether the right to the protection of personal data generally comprises some specific elements, or whether it does not. Similarly, it cannot be inferred that the EU right to the protection of personal data has been completely disconnected from the right to privacy in EU law. What needs to be stressed, in any case, is that the connection between EU personal data protection and privacy is contingent, and that it is not stable.

8.3.1 A Contingent Entanglement

The contingency of the coupling between privacy and personal data protection is demonstrated by the evolution of European personal data protection.[22] As shown, there are a number of Member States that historically have not envisaged the protection of personal data from the perspective of the right to privacy. It is a misconception, thus, to claim that the protection of personal data derives, generally speaking, from privacy.[23]

Even in the context of the Council of Europe, where the connection between personal data protection and the right to respect for private life took place mediated by the use of the word 'privacy' in Convention 108, this connection remains imperfect, and uncompleted.[24] In the framework of the EU, the reality is that the

[22] Supporting on the contrary the idea of an 'inherent' connection between personal data protection, respect for private life and privacy, see, for instance: (De Busser 2009, p. 21). Noting instead the need to question the conceptual validity of the instrumentality of data protection in relation to privacy: (Bygrave 2002, p. 8).

[23] That 'data protection' emerged from privacy or private life (Hijmans and Scirocco 2009, p. 1488), that 'data protection' is the offspring of privacy (Tzanou 2013, p. 88), or that it is the unwanted child of privacy (Safjan 2001, p. 27).

[24] Claiming nonetheless that personal data protection has acquired an autonomous status in the context of the Council of Europe, despite the lack of evidence in the case law of the ECtHR, which continues to frame any consideration of any data protection principles in the the application of

only EU-specific catalogue of fundamental rights recognised by EU law marks a distinction (even if qualified) between the respect to private life and personal data protection. Actually, the first manifestations of a right of individuals to access data about them surfaced in EU tentative listings on fundamental rights linking access to personal data not with the right to respect for private life, or privacy, but with the right to access public documents.

This connection between personal data protection and the right to access public documents is particularly telling, as it is through the path of a right to access data that various Latin American countries have designed the notion of a fundamental right to 'habeas data', that some regard as Latin America's interpretation of personal data protection.[25] Habeas data has been defined as the right of individuals to request access to files containing information about them, and to rectify inaccurate data; it sometimes applies only to public files,[26] and sometimes to both public and private ones, but remaining even then especially relevant for the access to public files (Ekmekdjian and Pizzolo 1996, p. 2).[27] The main difference between the concept of habeas data and the EU right to personal data protection is that the latter nowadays encompasses more than merely a subjective right to access data and to have data rectified, as it notably covers also a series of obligations for data processors, as well as independent supervision. Nonetheless, as evidenced by this research, European countries were originally also particularly concerned with the issue of automated data processing by public authorities, just like in the early steps of habeas data's evolution. The notion of habeas data acts thus a reminder of the fact that the genealogy of the EU right to the protection of personal data is not univocal.

8.3.2 An Unstable Connection

The surfacing of the EU right to the protection of personal data in EU law has been marked by various events of coupling and un-coupling with the right to privacy: although the disconnection was only exceptional until the entry into force of the Lisbon Treaty in December 2009, since then it has been acquiring more and more importance. The right's current status, namely as an emerging EU fundamental right to possibly supplant an ECHR right in the (human) rights anchorage of EU personal

Article 8 of the ECHR: (Bureau of the Consultative Committee of the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data 2013, p. 7).

[25] Or a third way, different from both European data protection and US privacy (see, for instance: (Guadamuz 2000). Formally, its Latin name echoes both a classical legal mechanism (habeas corpus), and the modernity of debates on regulation of data.

[26] See, for instance, Article LXXII(a) of the Brazilian Constitution.

[27] The Constitution of Argentina, for instance, enshrines since 1994 a right applicable primarily to data registered in public records or databases, and secondarily in private records or databases intended to supply reports (see Article 43 of the Constitution of Argentina). See, on this subject: (Ekmekdjian and Pizzolo 1996, especially p. 95).

data protection law, is particularly affected by a detachment from the right to privacy, or by the apparent move away from it.

This move, however, does not render privacy or private life irrelevant for the interpretation of EU personal data protection law. As already hinted, EU law currently conditions the interpretation of the right to personal data protection to the taking into account of legal instruments that refer to Article 8 of the ECHR. This provision is moreover deeply entrenched in the case law of the EU Court of Justice on EU personal data protection. Additionally, by taking the place of the right to privacy in the future EU data protection legal landscape, the right to personal data protection would also, in a certain way, reinforce its embroilment with (the spectre of) privacy. As noted, words are capable of acting upon the reading of law (and thus, also upon the construal of EU personal data protection law) not only by being explicitly present in the wording of legislation, but also when absent, in what can be described as a haunting presence.[28]

Legally, the adjective commonly used to underscore that law conceives of a right as separated from other rights is the term 'autonomous': rights can be regarded as such when they are applicable irrespective of another right's applicability. This autonomy of rights is not to be confused with the question of whether they are instrumental or not to the insurance of other rights, as ultimately all rights can arguably be envisaged as instrumental to the insurance of other rights, or of wider legal notions. From this viewpoint, the EU fundamental right to the protection of personal data has already functioned in EU law as an autonomous right, because it has been applied by the EU Court of Justice without any privacy-related grounding. Nonetheless, this does not mean that the right cannot be regarded as instrumental to the insurance or any other rights, including privacy, or that its understanding is not, in (legal) practice, conditioned by a legacy of interconnections with privacy.

In the literature, the portraying of personal data protection and privacy as equivalent legal terms is relatively widespread.[29] As a matter of fact, there is still a persistent tendency, especially among US scholars,[30] to refer to all rules in the field of data processing as 'privacy laws', which can actually led to inaccurate accounts of the current reality of EU law.[31] Presumably as a strategy to avoid the complexities of the question, 'data protection' and 'privacy' are also often simply mentioned jointly.[32]

---

[28] On EU personal data protection and the spectral presence of privacy, see also, for example: (González Fuster and Bellanova 2012).

[29] It can sometimes take the shape, for instance, of formulations such as 'data protection (privacy protection)' (Burkert 2009). Advancing that in many countries the concept of privacy has 'fused' with data protection: (Electronic Privacy Information Center (EPIC) and Privacy International (PI) 2007, p. 1).

[30] But not only among US scholars. For instance, stating that what has acquired a fundamental status 'in Europe' is 'information privacy': (Mayer-Schönberg 2010, p. 1862).

[31] Noting that the EU recognises 'privacy' as a fundamental right, but failing to make any reference to the fundamental right to the protection of personal data: (Schwartz and Solove 2013, especially p. 4).

[32] Observing that 'data protection' and 'privacy' are often mixed in calls for international instruments: (Kuner 2009, p. 308).

The limited number of authors that have attempted to determine what (intermittently) differentiates privacy from (personal) data protection[33] inevitably face the challenge of describing what can differentiate them. It is crucial, in this context, to avoid formulating the legal distinction between the two notions in terms that legal systems consider irrelevant, for instance by reintroducing into the conceptualisation of privacy, or of the respect for private life, a distinction between what is private and what is public, concretely in those legal systems where this distinction has been transcended. In reality, the disentanglement of privacy and personal data protection cannot only help to address personal data protection as only contingently attached to privacy, but also to embrace (or rediscover) the possibility of thinking of privacy in other terms, different from the personal data protection lens.[34]

The image of an overlap between privacy and (personal) data protection can be problematic, especially if it is understood as implying that, to the extent that they overlap, they are comparable or similar.[35] Some features of each legal notion might indeed be analogous, justifying the idea that conceptually they can be pictured as partially coincidental, but the reality is that at least in EU law the right to privacy and the right to personal data protection are configured differently, and protected differently. The former is protected across Europe as a human right enshrined in the ECHR, whereas the latter's insurance is still deeply dependent on the idiosyncrasies of its peculiar recognition by the EU Charter and the Lisbon Treaty. Therefore, the overlap between privacy and (personal) data protection might actually be more an illusion than a fact.

The fragility of existing conceptualisations of the right to the protection of personal data has recently become particularly visible in relation with the embryonic EU right to be forgotten. Discussions surrounding this concept highlight a lack of consensus not only on what could be the limits of the right to the protection of personal data, or its necessary arrangement with other fundamental rights, but also on the distinctions relevant for its design, and those irrelevant (i.e. does it make any difference for the right's applicability that personal data has been made *public*? or that the individual *consented* to its processing?). They also oblige to interrogate the limits of any conceptual equivalence between, on the one hand, current EU personal data protection and, on the other, any privacy envisaged in terms of (effective) control upon information.

---

[33] For instance, stressing an opposition between (US) privacy and (EU) data protection based on the latter's alleged correspondence with German informational self-determination: (Kuner 2004). Pointing out that already since Directive 95/46/EC EU personal data protection was not the same as 'informational privacy': (Brownsword and Goodwin 2012, p. 308). For a differentiation between privacy and private life: (Hildebrandt 2008, p. 311). Stating that the EU Charter addresses the fundamental right to personal data in a specific article 'quite confusingly': (Kokott and Sobotta 2013, p. 223).

[34] Highlighting that privacy shall not be reduced to personal data protection: (Poullet 2010, p. 28); noting a trend of monopolisation of privacy debates by data protection issues: (Gutwirth 2002, p. 2).

[35] As an example of the assertion according to which privacy and data protection 'plainly overlap': (Wacks 2010, p. 122). This idea of an overlap also seems to be behind the image of data protection and privacy as non-identical twins (De Hert and Schreuders Lyon 2001, p. 42).

8.4 Final Remarks

French philosopher Jacques Derrida claimed that philosophy requires getting rid of the authoritarian effects of language (Derrida 1998, p. 37). The present book was devoted to law, not philosophy, but has nonetheless also attempted to resist the disciplinarian effects of the language it uses. It has strived to observe the way in which EU law operates through language, and how language shapes, preserves, and alters (the meaning of) law (Kjaer 2004, p. 389).

The erasure of privacy proposed by the legislative package introduced by the European Commission in 2012 has not generated any major uproar. Privacy professionals and privacy commissioners, privacy forums and NGOs, privacy advocates and sceptics, privacy journals and conferences, both in Europe and across the Atlantic, in Brussels and elsewhere, have typically apprehended the proposals as privacy initiatives on the future of EU and global privacy, unaffected by the absence of the words that are not there. Re-formulated as 'contextual integrity' (Nissenbaum 2010, p. 231), permanently at risk (Rule 2007), finally understood (Solove 2008), appearing as the privileged punching ball of rising 'surveillance studies',[36] in creative 'privacy settings', or in the thousands of words of the multitude of 'privacy policies' that surround us, privacy is still very much present. The protection of personal data, in spite of its accredited status as emergent in EU law, might have just not emerged enough yet to counter this dominance, partially grounded on factors that go well beyond law. It has, however, managed to emerge in the face of it.

References

Alexy, Robert. 2010. *A Theory of Constitutional Rights (originally published 2002)*. Oxford: Oxford University Press.

Benjamin, Walter. 1992. *Illuminations*. London: Fontana Press.

Bennett, Colin J. 1997. Understanding ripple effects: The cross-national adoption of policy instruments for bureaucratic accountability. *Governance* 10 (3): 213–233.

Bennett, Colin J. 2011. In defense of privacy: The concept and the regime. *Surveillance & Society* 8 (4): 485–496.

Blanchot, Maurice. 1971. *L'amitié*. Paris: Gallimard.

Blanchot, Maurice. 1997. *Friendship (translated by Elizabeth Rottenberg)*. Stanford: Stanford University Press.

Brownsword, Roger, and Morag Goodwin. 2012. *Law and the Technologies of the Twenty-First Century: Text and Materials*. Cambridge: Cambridge University Press.

Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. 2013. Draft explanatory report of the modernised version of Convention 108 (based on the proposals adopted by the 29th Plenary Meeting of the T-PD). Council of Europe.

Burkert, Herbert. 1999. Privacy/data protection: A German/European perspective. In Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the

[36] See, for instance: (Lyon 2007, p. 171 ff) addressing jointly privacy and data protection). See also: (Bennett 2011).

Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass., 43–69. http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf.

Burkert, Herbert. 2009. Towards a new generation of data protection legislation. In *Reinventing Data Protection*?, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt. Dordrecht: Springer. Accessed 10 March 2013.

Bygrave, Lee A. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

Callon, Michel. 2006. Quatre modèles pour décrire la dynamique de la Science. In *Sociologie de la traduction*: *Textes fondateurs*, eds. Madeleine Akrich, Michel Callon, and Bruno Latour, 201–251. Paris: Écoles des mines de Paris.

De Busser, Els. 2009. *Data Protection in EU and US Criminal Cooperation: A substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*. Antwerpen: Maklu.

De Hert, Paul, and Eric Schreuders. 2001. The relevance of Convention 108. In Proceedings of the Council of Europe Conference on Data Protection, Warsaw 19–20 November 2001. Council of Europe.

Derrida, Jacques. 1998. *Le droit à la philosophie du point de vue cosmopolitique*. Lagrasse: Éditions Verdier.

Derrida, Jacques. 2004. Qu'est-ce qu'une traduction «relevante»? In *Cahier Derrida*, eds. Marie-Louise Mallet and Ginette Michaud. Paris: Éditions de l'Herne.

Ekmekdjian, Miguel Ánel, and Calogero Pizzolo. 1996. *Hábeas data: El derecho a la intimidad frente a la revolución informática*. Buenos Aires: Depalma.

Electronic Privacy Information Center (EPIC), and Privacy International (PI). 2007. Privacy & Human Rights 2006: An international survey of privacy laws and developments. Washington, D.C. and London: EPIC / PI.

Gómez Capuz, Juan. 2005. *La inmigración léxica*. Madrid: Arco Libros.

González Fuster, Gloria, and Rocco Bellanova. 2012. La protección de datos en Europa y la persistente huella de la privacidad. *NovATIca* 217:9–14.

Guadamuz, Andrés. 2000. Habeas Data: The Latin-American response to data protection. *The Journal of Information, Law and Technology (JILT)* 2. http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html. Accessed 10 March 2013.

Gutwirth, Serge. 2002. *Privacy and the Information Age*. Oxford: Rowman & Littlefield Publishers.

Gutwirth, Serge. 2007. Biometrics between opacity and transparency. *Annali dell'Istituto Superiore di Sanità* 43 (1): 61–65.

Gutwirth, Serge, and Paul De Hert. 2008. Regulating profiling in a democratic constitutional state. In *Profiling the European Citizen: Cross-disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth. Dordrecht: Springer.

Hijmans, Hielke, and Alfonso Scirocco. 2009. Shortcomings in EU data protection in the third and the second pillars: Can the Lisbon Treaty be expected to help? *Common Market Law Review* 46: 1485–1525.

Hildebrandt, Mireille. 2008. Profiling and the identity of the European citizen. In *Profiling the European Citizen: Cross-disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth, 303–343. Dordrecht: Springer.

Hornung, Gerrit. 2012. 'A general data protection regulation for Europe? Light and shade in the Commission's draft of 25 January 2012' SCRIPT-ed 64, 9 (1): 66–67.

Kjaer, Anne Lise. 2004. A common legal language in Europe? In *Epistemology and methodology of comparative law*, ed. Mark Van Hoecke, 377–398. Oxford: Hart Publishing.

Kokott, Juliane, and Christoph Sobotta. 2013. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law* 3 (4): 222–228.

Kruger, J. L. 2004. Translating Traces: Deconstruction and the Practice of Translation. *Journal of Literary Criticism, Comparative Linguistics and Literary Studies* 25 (1): 47–71.

Kuner, Christopher. 2004. Privacy, security and transparency: Challenges for data protection law in a New Europe. *European Business Law* 16 (1): 1–8.

Kuner, Christopher. 2009. An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review* 25: 307–317.

Luebke, David Martin, and Sybil Milton. 1994. Locating the victim: An overview of census-taking, tabulation technology, and persecution in Nazi Germany. *IEEE Annals of the History of Computing* 16 (3): 25–39.

Luhmann, Niklas. 1995. *Social Systems*. Stanford: Stanford University Press.

Luhmann, Niklas. 2012. *Theory of Society: Volume 1 (Translation by Rhodes Barrett)*. Stanford: Stanford University Press.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Mayer-Schönberg, Viktor. 2010. Beyond privacy, beyond rights—Toward a systems theory of information governance. *California Law Review* 98 (6): 1853–1886.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Pino, Giorgio. 2006. Il diritto all'identità personale ieri e oggi: Informazione, mercato, dati personali. In *Libera Circolazione e Protezione dei Dati Personali*, ed. Rocco Panetta. Milano: Giuffrè.

Poullet, Yves. 2010. About the e-Privacy Directive: Towards a third generation of data protection legislation? In *Data Protection in a Profiled World*, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert, 3–30. Dordrecht: Springer.

Purtova, Nadezhda. 2010. Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights. *Netherlands Quarterly of Human Rights* 28 (2): 179–198.

Rouvroy, Antoinette, and Yves Poullet. 2009. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In *Reinventing Data Protection*?, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 45–76. Dordrecht: Springer.

Rule, James B. 2007. *Privacy in Peril: How we are sacrificing a fundamental right in exchange for security and convenience*. Oxford: Oxford University Press.

Safjan, Marek. 2001. The right to privacy and personal data protection in the Information Society. In Council of Europe, Proceedings of the European Conference on data protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and future, 19 November, Warsaw.

Schwartz, Paul M., and Daniel J. Solove. 2013. Reconciling personal information in the United States and European Union. UC Berkeley Public Law Research Paper No. 2271442; GWU Legal Studies Research Paper No. 2013-77; GWU Law School Public Law Research Paper No. 2013-77. http://dx.doi.org/10.2139/ssrn.2271442.

Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge: Harvard University Press.

Tzanou, Maria. 2013. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law* 3 (2): 88–99.

Wacks, Raymond. 2010. *Privacy: A Very Short Introduction*. Oxford: Oxford University Press.

Wecksteen, Corinne. 2009. La traduction de l'emprunt: Coup de théâtre ou coup de grâce? *Lexis* 3: 137–156.