The Fundamental Right to Data Protection

Normative Value in the Context of Counter-Terrorism Surveillance

Maria Tzanou

• HART •
PUBLISHING
OXFORD AND PORTLAND, OREGON
2017

Hart Publishing
An imprint of Bloomsbury Publishing Plc

Hart Publishing Ltd
Kemp House
Chawley Park
Cumnor Hill
Oxford OX2 9PH
UK

Bloomsbury Publishing Plc
50 Bedford Square
London
WC1B 3DP
UK

www.hartpub.co.uk
www.bloomsbury.com

Published in North America (US and Canada) by
Hart Publishing
c/o International Specialized Book Services
920 NE 58th Avenue, Suite 300
Portland, OR 97213-3786
USA

www.isbs.com

First published 2017

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: HB: 978-1-50990-167-8
ePDF: 978-1-50990-168-5
ePub: 978-1-50990-169-2

Library of Congress Cataloging-in-Publication Data

Names: Tzanou, Maria, author.

Title: The fundamental right to data protection : normative value in the context of counter-terrorism surveillance / Maria Tzanou.

Description: Oxford [UK] ; Portland, Oregon : Hart Publishing, 2017. | Series: Modern studies in European law ; v. 71 | Includes bibliographical references and index.

Identifiers: LCCN 2016057792 (print) | LCCN 2016058889 (ebook) | ISBN 9781509901678 (hardback : alk. paper) | ISBN 9781509901692 (Epub)

Subjects: LCSH: Data protection—Law and legislation. | Terrorism—Prevention—Law and legislation.

Classification: LCC K3264.C65 T93 2017 (print) | LCC K3264.C65 (ebook) | DDC 342/.0662—dc23

LC record available at https://lccn.loc.gov/2016057792

Typeset by Compuscript Ltd, Shannon
Printed and bound in Great Britain by TJ International Ltd, Padstow, Cornwall

To find out more about our authors and books visit www.hartpublishing.co.uk. Here you will find extracts, author information, details of forthcoming events and the option to sign up for our newsletters.

Introduction

Καὶ μὴν καὶ τῶν πόνων πλείστας ἀναπαύλας τῇ γνώμῃ ἐπορισάμεθα, ἀγῶσι μέν γε καὶ θυσίαις διετησίοις νομίζοντες, ἰδίαις δὲ κατασκευαῖς εὐπρεπέσιν,ὧν καθ'ἡμέραν ἡ τέρψις τὸ λυπηρὸν ἐκπλήσσει.[1]

THIS BOOK INVESTIGATES the normative significance of data protection as a fundamental right in the European Union (EU). The Lisbon Treaty, which entered into force on 1 December 2009, elevated data protection to the status of a fundamental right as this was recognised in Article 8 of the European Union Charter of Fundamental Rights (EUCFR) alongside the right to privacy (Article 7 EUCFR). A substantial body of laws in the European Union—either general or sector-specific—pertains to data protection; however, the constitutional entrenchment of this as a fundamental right next to privacy, albeit welcomed in general with enthusiasm, raised the question of whether something had actually changed. In this context, the question normally goes: what is the added value of a right to personal data protection? Or to put it more simply, does it add anything to the right to privacy?

To answer these questions, the book explores the scope, the content and the capabilities of data protection as a fundamental right to resolve problems and to provide for effective protection. It identifies the limitations currently affecting this right that prevent it from having an added value of its own. Using a number of normative and structural arguments, the book reconceptualises our understanding of data protection so that it can operate as a fully fledged fundamental right.

It goes on to empirically test the reconstructed right to data protection in four case-studies of counter-terrorism surveillance. Surveillance is one of the main tools in the fight against terrorism, fundamental to the apprehension of terrorist networks and the prevention of terrorist attacks.[2] Surveillance is facilitated through the rapid advancement of new technologies and is often based on the co-operation of private actors compelled by law. Surveillance often targets personal information. This trend, also known as 'dataveillance', refers to the 'systematic monitoring

[1] Thoukidides: Pericles' Funeral Oration from the Peloponnesian War (Book 2.34–46), para 38. English translation available at http://hrlibrary.umn.edu/education/thucydides.html: 'Further, we provide plenty of means for the mind to refresh itself from business. We celebrate games and sacrifices all the year round, and the elegance of our private establishments forms a daily source of pleasure and helps to banish the spleen.'

[2] D Lyon, *Surveillance Society—Monitoring Everyday Life* (Celtic Court, Open University Press, 2001); M Tzanou, 'The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection' (2010) 4 *Vienna Online Journal of International Constitutional Law* 407.

of people's actions or communications through the application of information technology.'[3] The main purpose of dataveillance is to identify proactively 'risky groups'.[4] Dataveillance involves different aspects of individuals' everyday lives: their communications, their travel information, their financial information, their activities on the Internet.

This book analyses the normative significance of the reconstructed right to data protection in the context of four instances of EU counter-terrorism data surveillance: electronic communications metadata surveillance, travel data surveillance, financial data surveillance and Internet data surveillance. The surveillance case studies were selected for two main reasons. The first relates to the scope of application of the rights enshrined in the Charter. According to Article 51(1) EUCFR, the provisions of the Charter are addressed to the EU institutions, bodies, offices and agencies and to the Member States only when they are implementing EU law. While it has been generally accepted that Article 8 EUCFR can be applied horizontally,[5] it appears crucial to test the capabilities of this fundamental right, first and above all, in its vertical application to EU institutions and Member States' actions when they implement EU law. In this respect, data surveillance represents 'the broadest of the EU's actions to counter terrorism.'[6] Indeed, EU counter-terrorism law largely concerns the collection and exchange of personal data[7] that affect in an indiscriminate manner almost every person in the EU. This leads to the second reason: the effects of EU data surveillance measures are particularly significant, thus, making it imperative to investigate the normative significance of the fundamental right to data protection in this context. In essence, the study of data surveillance measures in the light of the fundamental right to data protection aims to test the legal bite of this right in the most difficult context. The empirical chapters of the book follow a common structure that both reflects a discussion of the normative value of the fundamental right to data protection in each particular context of data surveillance, and provides a substantive counter-terrorism analysis of the specific measures examined against the fundamental rights to privacy and data protection.

The book, which bridges the gap between EU constitutional data protection law and counter-terrorism law, is divided into two parts. Part I reflects on the extent to which data protection can operate as a fully fledged fundamental right. Part II

[3] R Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (1988) 31(5) *Communications of the ACM* 498.

[4] M Levi and D Wall, 'Technologies, Security and Privacy in the post 9/11 European Information Society' (2004) 31 *Journal of Law and Society* 194, 200.

[5] E Frantziou, 'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality' (2015) 21(5) *European Law Journal* 657, 660; E Spaventa, 'The horizontal application of fundamental rights as general principles of Union Law', in A Arnull et al (eds) *A constitutional order of states: essays in honour of Alan Dashwood* (Oxford, Hart Publishing, 2011) 199.

[6] C Murphy, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Oxford, Hart Publishing, 2012) 147.

[7] See V Mitsilegas, *EU Criminal Law* (Oxford, Hart Publishing, 2009) ch 5; V Mitsilegas and A Baldaccini, 'Interdependence of the various initiatives and legislative proposals in the fields of Counter-terrorism and police co-operation at the European level', Briefing Note requested by the European Parliament's LIBE Committee, October 2007, 11.

informs the theoretical discussion on the added value of the fundamental right to data protection by empirically examining, in the light of this right, four case studies of EU counter-terrorism data surveillance. '*Ratione temporis*' the study presents the legal framework until the end of September 2016.

Part I lays down the theoretical and analytical framework of the analysis and consists of the first two chapters. Chapter 1 brings clarity to the concepts of privacy and data protection and considers the differences between them. It situates data protection in the context of EU constitutionalism and human rights law by paying special attention to its initial conception as a factor that would permit the free movement of data rather than a fundamental human right. It examines the foundational values and aims of the fundamental right to data protection and argues that these transcend privacy. It discusses the current approaches in the legal scholarship and the case law on data protection, and identifies their shortcomings. It then develops a theory on data protection that reconstructs this right and shapes its understanding in a clear and comprehensive manner that can guide courts and legislators on data protection issues.

Chapter 2 examines the jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU or ECJ, used interchangeably) on the right to data protection. The ECtHR in a series of judgments has recognised data protection as an aspect of the right to private and family life found in Article 8 ECHR. Data protection has been the subject-matter of a rich case law of the CJEU even before its constitutional entrenchment as a fundamental right by the Lisbon Treaty. However, the Court's jurisprudence regarding data protection has significantly developed since that point. In the initial years after the inclusion of this right in the Charter, the Court, while aware of its existence, could not disassociate it from privacy. Subsequently, it reluctantly started to distinguish the two rights, and recent decisions illuminate that it has reached its maturity regarding the assessment of data protection. However, it is argued that there are still outstanding issues in the Court's analysis of this fundamental right that raise confusion as to its content and impede its functionality.

Part II examines the normative significance of the reconstructed fundamental right to data protection in different instances of counter-terrorism data surveillance. Chapter 3 considers the case of communications metadata surveillance. Communications metadata refers to information that can reveal the equipment, the location, the time and the participants of a communication, but not its content. The analysis examines the EU Data Retention Directive that imposed an obligation on electronic communications service providers to retain such data in order to fight terrorism and serious crime. The Directive was invalidated by the Court of Justice in its landmark decision in *Digital Rights Ireland*,[8] but the issue of metadata retention has not been resolved, since Member States have maintained or reintroduced such legislation at the domestic level.

[8] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2014] ECR I-238.

Chapter 4 focuses on travel data surveillance and examines the Passenger Name Record (PNR) case. This has both an international aspect, as the EU has entered into several bilateral international agreements on the transfer of PNR data, and a domestic one, as the EU has recently adopted its own PNR system. The chapter discusses the EU-US PNR saga and the EU PNR system. It analyses the context and content of these measures as well as the institutional actors involved in their adoption. It provides an overview of US privacy law and highlights its major shortcomings. It assesses the EU-US 'Umbrella' Agreement in the field of law enforcement and the recently adopted Judicial Redress Act of 2015, and finds that these do not provide robust protection of personal data on the other side of the Atlantic. It argues that the PNR case study is a prime example of the normative added value of a reconstructed fundamental right to data protection and demonstrates why the conceptual confusions of privacy and data protection often committed by the European judiciary are not merely theoretically erroneous, but also dangerous in practice. The chapter also reflects on the issues raised by terrorist profiling and concludes with a substantive fundamental rights assessment of the PNR.

Chapter 5 discusses financial data surveillance by considering the Terrorist Finance Tracking Programme (TFTP). It analyses how the programme became the subject of an international agreement between the EU and the US after its initial secret operation. It investigates the problematic role of Europol in the context of the EU-US TFTP Agreement and discusses the implications of the programme in the light of the fundamental rights to privacy and data protection.

Chapter 6 focuses on the Internet data surveillance undertaken by the US intelligence authorities as revealed by Edward Snowden. It examines the US foreign intelligence surveillance measures carried out with the compulsory assistance of leading US-based Internet companies such as Facebook, Skype, Google, Microsoft and Apple, and analyses the CJEU's seminal decision in *Schrems*[9] that invalidated the Safe Harbour scheme. It assesses the recently adopted Privacy Shield in the light of fundamental rights and concludes that this does not comply with the Court's pronouncements regarding the permissibility of mass surveillance targeting the content of electronic communications.

Chapter 7, Conclusions, draws together the discussion and addresses the core questions of whether and how the fundamental right to data protection can have a normative significance in the context of counter-terrorism data surveillance. While it is argued that the reconstructed right to data protection has an added value in the substantive assessment of counter-terrorism measures, the case studies suggest that modern surveillance techniques can empty essential aspects of the content of this right to the detriment of the data subjects. The book submits that it is in these cases that the essence of the fundamental right to data protection should be able to play a role and calls for the Court of Justice to develop its case law in this direction.

[9] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Judgment of the Court (Grand Chamber), 6 October 2015).

decisions.'[66] In this respect, the control over personal information conception of privacy is narrow because it fails to take the second interest into account. On the other hand, it is too vague because it does not provide a clear definition of the notion of personal information, over which the individual is entitled to control.[67] For instance, while one definition of personal information as 'control over who can see us, hear us, touch us, smell us, and taste us, in sum, control over who can sense us',[68] is considered unduly broad; another, that sees personal information as 'any data about an individual that is identifiable to that individual'[69] does not fit well in a privacy theory, because 'there is a significant amount of information identifiable to us that we do not deem as private'.[70]

II. CONCEPTUALISING DATA PROTECTION

Writing on the concept of data protection, Paul de Hert and Serge Gutwirth comment that 'it is impossible to summarise data protection in two or three lines. Data protection is a catch-all term for a series of ideas with regard to the processing of personal data'.[71] Directive 95/46/EC (the 'European Data Protection Directive' or 'Data Protection Directive')[72] considers data protection as the protection of 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'[73] The General Data Protection Regulation (GDPR),[74] which repeals the Data Protection Directive and which will apply from 25 May 2018, states that it 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'[75] The notions of 'processing' and 'personal data' are central to understanding the concept of data protection. In general terms, 'processing' can be

[66] ibid, 762. *See* also *Whalen v Roe* 429 US 589 (1977), 598–600.

[67] Solove, n 15 above, p 24.

[68] RB Parker, 'A Definition of Privacy' (1974) 27 *Rutgers Law Review* 275, 280.

[69] RS Murphy, 'Property Rights in Personal Information: An Economic Defence of Privacy' (1996) 84 *Georgetown Law Journal* 2381, 2383.

[70] Solove, n 15 above, p 25.

[71] P de Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S Gutwirth and others (eds), *Reinventing Data Protection?* (New York, Springer, 2009) 3.

[72] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/3, (Data Protection Directive).

[73] Data Protection Directive, Art 1(1). Similarly, Convention No 108 of the Council of Europe defines data protection as 'the respect of the rights and freedoms [of the individual], and in particular his right to privacy, with regard to automated processing of personal data relating to him'. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No 108.

[74] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L119/1.

[75] GDPR, Art 1(2). See also Art 1(1).

seen as any operation performed upon the data, from their collection, recording, storage, use, to their disclosure, dissemination, erasure and destruction.[76] The data are considered personal, when they can be linked to a certain individual, normally referred to as the 'data subject'.[77] Data protection can be conceived, thus, as referring to this set of legal rules that aim to protect the rights, freedoms and interests of individuals, whose personal data are collected, stored, processed, disseminated, destroyed, etc.[78] The rights granted to the 'data subjects' correspond to relevant responsibilities of the 'controllers'. 'Controllers' are the natural or legal persons who 'determine the purposes and means of the processing of personal data'.[79]

The ultimate objective of data protection is to ensure 'fairness in the processing of data and, to some extent, fairness in the outcomes of such processing'.[80] The fairness of processing is safeguarded by a set of principles (also known as 'fair information principles' or 'data protection principles'), which, in general terms, can be couched as follows:[81]

1) personal information should be collected and processed fairly and lawfully;
2) it should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
3) it should be adequate, accurate, relevant and not excessive with regard to the purposes for which it is collected and processed;
4) it should not be kept for longer than is necessary for the purposes for which it was collected and processed;
5) the consent of the person to whom the information relates is necessary for some categories of processing;
6) security measures should be taken in order to protect the data from accidental loss or unauthorised disclosure and use;
7) the individual should be informed that his/her data are held by others; should be given access to them and the possibility to correct them and delete them in certain cases;
8) the processors of personal information should be accountable for complying with the fair information principles;
9) compliance with these requirements should be controlled by an independent authority.

[76] See Data Protection Directive, Art 2(b); Art 4(1) GDPR and Art 2(c) of Convention 108.

[77] Data Protection Directive Art 2(a) provides that 'personal data' denotes 'any information relating to an identified or identifiable natural person'. See also Art 4(1) GDPR and Art 2(c) of Convention 108.

[78] F Hondius, *Emerging Data Protection in Europe* (New York, American Elsevier, 1975) 1.

[79] Data Protection Directive, Art 2(d) and Art 4(7) GDPR. Art 2(d) of Convention 108 uses the concept 'controller of the file'.

[80] Bygrave, n 32 above, p 168.

[81] The list presents indicatively only a core of fair information principles. The exact formulation of the principles differs in the various texts, for instance, the EU Data Protection Directive, the GDPR, the CoE Convention No 108, the OECD and the APEC privacy guidelines. See also Art 29 WP, Transfers of personal data to third countries: Applying Arts 25 and 26 of the EU Data Protection Directive, 24 July 1998, 5.

While defining data protection does not seem to involve the philosophical controversies and difficulties that the concept of privacy faces, nevertheless, it is not a notion without problems itself. Its meaning is not very clear from the outset,[82] all the more because its definition appears to be quite technical and confusing, as it is based on further concepts, such as 'personal data' and 'processing' that seek definition themselves.[83] The term 'data protection', which is derived from the German *Datenschutz*, is most commonly used in (continental) European jurisdictions; in the USA, Canada and Australia, other terms such as 'informational privacy', 'data privacy' or simply 'privacy protection' are used.[84]

A. Approaches to Data Protection

There is often a confusion at to how data protection should be perceived. Is data protection a factor of economic growth? Is it a fundamental human right? Is it a consumer right?[85] Or can it be simply seen as a 'problem of trust' over the security of personal information?[86] There are different ways of approaching data protection[87] and the debate is not without practical consequences for the concept of the notion. Below, the two main approaches to data protection, the economic approach and the fundamental rights' approach are discussed. The OECD privacy regulatory framework is used as an example of the former, and that of the EU as an example of the latter.[88]

i. The Economic Approach

An example of the economic approach to data protection can be found in the OECD Privacy Guidelines. The Organisation for Economic Co-operation and

[82] *Contra* Hondius who argues that 'Etymologically, … the term [data protection] is not quite correct, but its meaning is clear.' Hondius, n 78 above, p 1.

[83] The term data protection has also been criticised for concentrating disproportionately on the data rather than the person as the object of protection. See Bennett and Raab, n 11 above, p 11; L Bygrave, *Data Privacy Law—An International Perspective* (Oxford, Oxford University Press, 2013) 23.

[84] Bygrave, n 32 above, p 1.

[85] This approach is followed in the APEC Privacy Framework, www.dpmc.gov.au/privacy/apec/apec_privacy_framework.cfm. The Framework contains nine Privacy Principles: 1) Preventing Harm; 2) Notice; 3) Collection Limitations; 4) Uses of Personal Information; 5) Choice; 6) Integrity of Personal Information; 7) Security Safeguards; 8) Access and Correction; and 9) Accountability. See also, CD Terwangne, 'Is a Global Data Protection Regulatory Model Possible?' in S Gutwirth and others (eds), *Reinventing Data Protection?* (New York, Springer, 2009) 175, 181, 183–85.

[86] This was the approach adopted by the World Summit on the Information Society in its Declaration of Principles (Declaration of Principles—Building the Information Society: a global challenge in the new Millennium, Document WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003). According to this approach, data protection coincides with data security, and security breaches are the problems to be dealt with.

[87] For an analysis of the different regulatory regimes worldwide see AL Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Ithaca, Cornell University Press, 2008).

[88] It should be noted that the two approaches are not mutually exclusive; on the contrary, they are often both present at the same time in legal documents.

Development (OECD) is an international organisation established in 1961, whose aim is to promote policies to improve economic and social well-being. It is an economic organisation that measures productivity and global flows of trade and investment, carries out analysis mainly in economic matters, and is not involved in human rights activities. It attempts to promote rules and set international standards in many areas, such as, for instance, development, education, employment, energy, environment, finance, investments, science and technology, taxation and trade.

In a symposium organised by the OECD in 1977 on Transborder Data Flows and the Protection of Privacy, the economic value and national interest of transborder data flows was discussed by the participants. In a comment made by Louis Joinet,[89] who participated later in the drafting of the OECD Guidelines, it was noted:

> Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows.[90]

Following the symposium, an Expert Group[91] was created to begin work on the privacy guidelines. The main aim was to tackle concerns about the growing use of personal data and computerised processing. But, given the OECD's mandate to promote economic growth and contribute to the expansion of world trade, a further aim was to prevent national laws from creating barriers to the free flow of information[92] and to the development of economic and social relations among member countries.[93] The Guidelines, adopted on 23 September 1980,[94] place an emphasis on ensuring that the measures introduced to protect personal data would not result in restricting transborder data flows. Thus, data protection is

[89] Louis Joinet was at the time the President of the French *Commission nationale de l'informatique et des libertés* (CNIL) (National Commission on Informatics and Liberty).

[90] Louis Joinet as quoted in J Eger, 'Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non- Tariff Barriers?' (1978) 10 *Law and Policy in International Business* 1065, 1066.

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

[92] See Working Party on Information Security and Privacy, 'The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines', OECD Digital Economy Paper, 30 April 2011, www.oecd.org/officialdocuments/displaydocumentpdf/?cote=dsti/iccp/reg(2010)6/final&doclanguage=en.

[93] See OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), available at www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.

[94] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html. The OECD Privacy Guidelines are not legally binding. The Guidelines contain eight fair information principles: 1) the Collection Limitation Principle; 2) the Data Quality Principle; 3) the Purpose Specification Principle; 4) the Use Limitation Principle; 5) the Security Safeguards Principle; 6) the Openness Principle; 7) the Individual Participation Principle; and 8) the Accountability Principle.

seen mainly as a factor fostering international economic aims through the facilitation of free and unimpeded transfers of personal information.[95]

ii. The Fundamental Rights' Approach

The European Union constitutes the prime example of the fundamental rights approach to data protection.[96] Unlike the Council of Europe, the EU is not a human rights organisation. It was created as an economic community, and while it has gone a long way from that, still, many of its competences are of an economic nature.

Data protection, hence, at its birth in the EU, was an internal market concern, similar to the economic approach of the OECD Guidelines analysed above. Directive 95/46/EC, the 'Data Protection Directive', was the first piece of legislation adopted in the EU on the protection of personal data.[97] The Directive had two objectives: to harmonise the different national rules on data protection, and to ensure simultaneously the free movement of such data.[98] Fundamental rights and market freedoms were placed on the same footing under the Directive.[99] According to Recital 3, the establishment and functioning of the internal market in which goods, persons, services and capital can move freely requires 'not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.' This was because divergent levels of protection of fundamental rights, and in particular of the right to privacy with regard to the processing of personal data, would create obstacles to the pursuit of a number of economic activities at Community level.[100] In order to remove these obstacles, the level of protection of individual rights had to be made equivalent in all Member States.[101] The equivalent protection of fundamental rights was expected to render free movement of data possible because

[95] See S Nouwt, 'Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union' in S Gutwirth and others (eds), *Reinventing Data Protection?* (New York, Springer, 2009) 275, 278.

[96] Data protection is recognised as a fundamental right at the constitutional level in several European countries, such as Portugal, Austria, Spain, Greece, Hungary, Slovakia, the Czech Republic, Poland and Estonia.

[97] For an analysis of the EU legal framework see M Tzanou, 'Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence' in C Akrivopoulou and A Psygkas (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices* (Hershey, IGI Global, 2011) 273; M Tzanou, 'Data Protection in EU Law after Lisbon: Challenges, Developments, and Limitations' in M Gupta (ed) *Handbook of Research on Emerging Developments in Data Privacy* (Hershey, IGI Global, 2014) 24.

[98] Data Protection Directive, Art 1.

[99] This is also evident in the title of the directive: '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.' See S Gutwirth, *Privacy and the Information Age* (Oxford, Rowman & Littlefield Publishers, 2002) 91–92; L Bergkamp, 'EU Data Protection Policy—The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' (2002) 18 *Computer Law and Security* 31, 33 and 37.

[100] Data Protection Directive, Recital 7.

[101] Data Protection Directive, Recital 8.

Member States would 'no longer be able to inhibit the free movement between them of personal data on grounds relating to the protection of the rights and freedoms of individuals, and in particular the right to privacy.'[102] The Directive was, thus, intended as a harmonisation instrument and was adopted under the legal base of Article 95 of the EC Treaty (now Article 114 TFEU), which concerns the approximation of legislation relating to the internal market.

Data protection was not only born out of internal market concerns; its concept was also recognised as a dimension of privacy and its protection was dependent on it. According to the Data Protection Directive:

> the object of the … laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the ECHR and the general principles of Community law.[103]

Data protection was included as a fundamental right in the EUCFR, which enjoys the status of EU primary law pursuant to Article 6(1) TEU,[104] since the Lisbon Treaty entered into force as from 1 December 2009. The relevant provision is Article 8 EUCFR. The right to privacy is enshrined in the Charter in Article 7 EUCFR, which 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.

Article 8 of the Charter provides:

> *Article 8—Protection of personal data*
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access 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.

The fundamental right to personal data protection is set out in three paragraphs in Article 8 EUCFR. The first contains the general recognition of the right: everyone has the right to the protection of personal data concerning him or her. The second and the third paragraphs describe the content of the right and lay down six requirements applicable to the processing of personal data.[105] Personal data:

[102] Data Protection Directive, Recital 9.

[103] Data Protection Directive, Recital 10. Art 1 of the Directive stipulates: 'Member States 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.'

[104] Consolidated Version of the Treaty on European Union [2008] C326/15 (TEU), Art 6(1) TEU provides: 'The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.'

[105] González Fuster, n 33 above, p 4.

1) must be processed fairly; 2) for specified purposes; 3) on the basis of the consent of the person concerned or some other legitimate basis laid down by law; 4) individuals must have a right to access data concerning them; 5) a right to rectify it; and 6) compliance with these rules must be subject to control by an independent authority. All six requirements correspond to respective data protection principles: 1) the principle of fair processing; 2) the principle of purpose specification; 3) the need of a legitimate basis for processing; 4) the right of access; 5) the right of rectification; and 6) the principle of independent supervision.

The inclusion of data protection in the EUCFR signals the EU's departure from an economic approach to data protection to a fundamental rights' one for two reasons: first, data protection is formally recognised as a fundamental right in primary EU constitutional law,[106] and second, for the first time at the international level, data protection is disassociated from the right to privacy, in that it is no longer regarded as a fundamental right, insofar as it can be seen as an aspect of privacy.

B. Data Protection as a Fundamental (Human?) Right

Human rights scholars normally agree that 'there are no inherent reasons' explaining why new human rights should not be recognised in international law.[107] Nonetheless, the recognition of new human rights must be able to achieve a balance between, on the one hand, 'the need to maintain the integrity and credibility of the human rights tradition', and on the other hand, 'the need to adopt a dynamic approach that fully reflects changing needs and perspectives and responds to the emergence of new threats to human dignity and well-being.'[108] In this sense, it has been suggested that a certain claim should satisfy a number of criteria in order to qualify as a human right in terms of international law. There is not a unique, authoritative list of criteria, but most commonly these have been set out in the following way.[109] The new human right should: a) 'reflect a fundamentally social value'; b) be relevant in diverse value systems; c) be eligible for recognition on the basis that it is an interpretation of international law obligations or a formulation that is declaratory of general principles of law; d) 'be consistent with, but not merely repetitive of, the existing body of international human rights law'; e) be

[106] Data protection is also enshrined in Arts 16 TFEU and 39 TEU. See H Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Switzerland, Springer International Publishing, 2016).

[107] P Alston, 'Making Space for New Human Rights: The Case of the Right to Development', (1988) 1 *Harvard Human Rights Year Book* 3, 39.

[108] P Alston, 'Conjuring up New Human Rights: A Proposal for Quality Control' (1984) 78 *American Journal of International Law* 607, 609.

[109] The list of criteria is adapted from the relevant list provided by Alston regarding the recognition of new human rights in international law. Alston, n 108 above, p 615.

capable of achieving a very high degree of consensus; and f) 'be sufficiently precise as to give rise to identifiable rights and obligations'.[110]

While international law instruments normally use the term 'human rights', the EU (and national legal orders) speak of 'fundamental rights'. Fundamental rights are defined as 'rights contained in a constitution or in a certain part of it, or if the rights in question are classified by a constitution as fundamental rights'.[111] The explicit recognition of an EU bill of rights, the EU Charter of Fundamental Rights has its own history. Although fundamental rights were recognised and protected as general principles of EU law by the ECJ, the EU did not have a written text of rights. Discussions for the adoption of an EU list of fundamental rights started in the 1980s. Following the adoption of the Amsterdam Treaty, the Commission appointed a 'Group of Experts' to assess the opportunities and constraints of an explicit recognition of fundamental rights, including the introduction of new rights mirroring the 'challenges of an information society'.[112] The Group of Experts concluded that 'a text enabling individuals to ascertain their rights' was 'imperative for *affirming* fundamental rights in the European Union'.[113] In June 1999, the Cologne European Council decided that a 'Charter of Fundamental Rights' should be established in the EU in order to make the overriding importance and relevance of fundamental rights 'more visible to the Union's citizens'.[114] The elaboration of the drafting of the Charter was assigned to a body composed of representatives of the Heads of State and Government, the President of the Commission, Members of the European Parliament and national parliaments.[115] The body, which named itself 'the Convention', officially concluded the draft of the Charter on 2 October 2000. The Charter of Fundamental Rights of the EU was formally proclaimed by the EU institutions on 7 December 2000[116] and became legally binding with the entry into force of the Lisbon Treaty on 1 December 2009.

The Charter's preamble states that 'it is necessary 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*.'[117] In fact, according to the preamble, the Charter 'reaffirms' fundamental rights as they result from 'the constitutional traditions and international obligations common to the Member States', the EU Treaties, the ECHR, the Social Charters adopted by the Community and by the Council of Europe and the case law of the Court of Justice

[110] ibid.

[111] R Alexy, 'Discourse Theory and Fundamental Rights' in Agustín José Menéndez and Erik Oddvar Eriksen (eds), *Arguing Fundamental Rights* (Dordrecht, Springer, 2006) 15.

[112] Expert Group on Fundamental Rights, *Affirming Fundamental Rights in the European Union: Time to Act* (Brussels: European Commission, 1999) 6.

[113] ibid, p 13. Emphasis added.

[114] Cologne European Council, 3–4 June 1999, Conclusions of the Presidency, Annex IV—European Council Decision on the drawing up of a Charter of Fundamental Rights of the European Union.

[115] ibid.

[116] Charter of Fundamental Rights of the European Union proclaimed on 7 December 2000 in Nice ([2000] OJ C364/1). For a commentary on the Articles of the Charter, see EU Network of Independent Experts on Fundamental Rights, 'Commentary of the EU Charter of Fundamental Rights', 2006.

[117] Preamble to the Charter of Fundamental Rights. Emphasis added.

of the European Communities and of the European Court of Human Rights.[118] The Explanations to the Charter[119] state that the right to the protection of personal data is based on Article 286 EC, Directive 95/46/EC, Article 8 ECHR and Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data. This pronouncement appears confusing for several reasons. First, Article 8 ECHR establishes the right to respect for private and family life, but does not mention data protection. Second, Directive 95/46/EC constitutes secondary EU law and does not fall within any of the fundamental rights sources mentioned in the Charter's preamble. Thirdly, Convention 108 refers to data protection as safeguarding respect for 'the rights and fundamental freedoms of the individual, and in particular his right to privacy, with regard to automatic processing of personal data relating to him'.[120] Data protection is, therefore, associated with privacy in that instrument, and is not recognised as a fundamental right as such.[121] Finally, Article 286 EC (now replaced by Article 16 TFEU) was the Treaty legal basis ensuring that Community institutions and bodies were bound by data protection legislation under the supervision of an independent body. Article 286 EC, while primary law, did not establish a fundamental right to the protection of personal data as the one recognised by Article 8 EUCFR. It seems, therefore, that the Charter has done much more than simply 'reaffirming' data protection as a right found in other sources; the Charter has introduced a new fundamental right, albeit with an already familiar content. The recognition of data protection as a fundamental right in the EU seems to broadly satisfy the criteria employed by international human rights scholars for the introduction of new human rights: data protection reflects fundamental social values in the era of the rapid advancement of new technologies; it has been relevant for some time in national, international and transnational systems; it is consistent with the existing body of laws in the field; it achieved a high degree of consensus at least in the EU; and it gives rise to 'identifiable rights and obligations'.

As to why data protection was recognised as a fundamental right in the EU, academic literature has identified three possible explanations. First, the European Union, 15 years after the Data Protection Directive, is more than an economic union, as its name implies. Its competences extend to Common Foreign and Security Policy (CFSP)—the former Second Pillar, and Police and Judicial Cooperation in Criminal Matters (PJC)—the former Third Pillar.[122] Data protection had, therefore, to be distanced somehow from internal market freedoms in order

[118] ibid.

[119] On the interpretative value of the explanations of the Charter, see K Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 *European Constitutional Law Review*, 375, 401–02.

[120] Art 1 Convention No 108.

[121] See D Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (Chapel Hill, University of North Carolina Press, 1989) xiv.

[122] The shortcomings of fundamental rights protection in the second and third pillars were identified by the Group of Experts also as reasons for the elaboration of a written text of fundamental rights in the EU.

to cover those areas.[123] Data protection as a fundamental right applies to further areas of processing, besides the common market and the commercial flows of personal data. Data protection is made, thus, 'a legal requirement throughout the Union'[124] and covers processing for law enforcement purposes.[125] Second, the time seemed ripe for the 'independence' of data protection from privacy.[126] A fundamental right to data protection expresses values that go beyond privacy.[127] In this respect, some authors have also pointed out that the recognition of a separate right to data protection, next to privacy, is 'more respectful of the different European constitutional traditions',[128] because it takes into account that certain EU Member States, for instance, Germany and France, do not link data protection to privacy, but base it on different constitutional values, such as liberty (France) or dignity and personality (Germany).[129] Finally, there is a pragmatic reason for the elevation of data protection to the status of a fundamental right: individuals must be aware of its existence and conscious of the ability to enforce it in the light of the new challenges arising from the rapid development of information and communication technologies.[130]

C. A Complicated Relationship: Data Protection and Privacy

Following the constitutional entrenchment at the EU level of a right to data protection, the exact nature of the relationship between privacy and data protection has been the subject of a vivid academic debate. In particular, legal scholars have been concerned with the question whether data protection can be conceived as a 'separate'[131] or an 'autonomous'[132] fundamental right, 'distinct'[133] from the right

[123] In its First Report on the Implementation of the Data Protection Directive, the Commission notes that Art 8 EUCFR 'has given added emphasis to the fundamental rights dimension of the Directive.' See Commission, 'First report on the implementation of the Data Protection Directive (95/46/EC) (Data Protection)', COM(2003) 265.

[124] Art 29 WP on the Protection of Individuals with Regard to the Processing of Personal Data, Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights.

[125] Nouwt, n 95 above, p 286.

[126] De Hert and Gutwirth note that the recognition of a constitutional right to data protection in the EU Charter 'allows for a sensible constitutional division of labour.' P De Hert and S Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in Erik Claes et al (eds), *Privacy and the Criminal Law* (Antwerpen, Intersentia, 2006) 61, 81.

[127] Art 29 WP, Opinion 4/2007 on the concept of personal data. For an overview of the values see below.

[128] De Hert and Gutwirth, n 126 above, p 82.

[129] See P Schwartz and KN Peifer, 'Prosser's Privacy and the German Right of Personality: Are Four Torts Better than One Unitary Concept?' (2010) 98 *California Law Review* 1925, 1946.

[130] See EU Network of Independent Experts on Fundamental Rights, n 116 above, p 11.

[131] N Scandamis, F Sigalas and S Stratakis, 'Rival Freedoms in Terms of Security: The Case of Data Protection and the Criterion of Connexity', (2007) CEPS, CHALLENGE, Research Paper No 7, 15.

[132] S Rodotà, 'Data Protection as a Fundamental Right' in S Gutwirth et al (eds), *Reinventing Data Protection?* (New York, Springer, 2009) 79.

[133] G González Fuster, P De Hert and S Gutwirth, 'The Law-Security Nexus in Europe: State-of the-Art report' (INEX, 2008) 10.

to privacy, or whether it should be regarded as an aspect of privacy. The confusion is further exacerbated by the fact that data protection is often referred to as 'informational privacy', 'data privacy' or simply 'privacy', especially on the other side of the Atlantic. Furthermore, it has been argued that it is not clear whether privacy and data protection 'overlap'[134] in certain aspects, so that they can be seen as 'similar' rights.[135]

A number of points can be advanced here. First, one cannot lose sight of the EU constitutional reality: data protection has been recognised as a fundamental right, alongside privacy in the EU Charter of Fundamental Rights, which constitutes primary EU law. This means that, in the European constitutional landscape at least, data protection is considered (or expected) to add something to privacy. Whether this is the case, in the context of counter-terrorism surveillance, is a question that the present book explores.

Second, one cannot lose sight of the historical reality: data protection legislation is a relative newcomer; it only appeared in Member States' legislation in the 1970s as a response to the concerns raised about the increasingly centralised processing of personal data and the establishment of huge data banks.[136] The first piece of data protection legislation was enacted in 1970 by the German state of Hesse.[137] It was followed by Sweden in 1973[138] and, subsequently, by other European countries.[139] In most cases, legislators opted to legitimise the data protection regulation by simply referring to traditional privacy concepts.[140] As has been pointed out, 'provisions proclaiming the right to privacy or private life constitute the most direct inspiration for the principles of data protection laws.'[141] On the other hand,

[134] R Wacks, *Privacy: A Very Short Introduction* (Oxford: Oxford University Press, 2010) 122.

[135] G González Fuster, n 33 above, p 271 and references therein. It is not clear, however, what the meaning of 'similar' rights is and what is the normative significance of such characterisation.

[136] For a detailed account on the history of the emergence of data protection laws in national and international legal orders, see G González Fuster, n 33 above; O Lynskey, *The Foundations of EU Data Protection Law* (Oxford, Oxford University Press, 2016); Bygrave, n 32 above, p 93; S Simitis, 'New Developments in National and International Data Protection Law in Recent Developments' in J Dumortier (ed), *Data Privacy Law: Belgium's Data Protection Bill and the European Draft Directive* (Leuven, Leuven University Press, 1992) 1, 22.

[137] *Datenschutzgesetz*, 7 Oct 1970, § 6, 1 *Gesetz- und Verordnungsblatt für das Land Hessen* 625 (1970). For the history and development of the law, see S Simitis, 'Datenschutzrecht' in Hans Meyer and Michael Stolleis (eds) *Hessisches Staats- und Verwaltungsrecht (HESSSTVWR)* (2nd edn) (Baden-Baden, Nomos, 1986) 111, 114.

[138] *Datalagen* (Swedish Data Act) of 11 May 1973, entered into force 1 July 1973.

[139] Austria (Federal Act of 18 October 1978 on the protection of personal data, *Bundesgesetzblatt* No 565/1968); Denmark (Public Authorities Registers Act, No 294 (1978), and Private Registers Act No 293 (1978)); France (Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, [1978] JO 227); West Germany (Federal Data Protection Act [1977] BGB1 I 201); Norway (Act of 9 June 1978 relating to Personal Data Registers).

[140] Simitis, n 50 above, p 730.

[141] Bygrave, n 32 above, p 116. However, González Fuster contends that it is a 'misconception' to argue that data protection derives from privacy, because '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.' See G González Fuster, n 33 above, p 268.

to rephrase Spiros Simitis, privacy is 'an old and venerable'[142] right, entrenched for many years as a fundamental right in national constitutions and international texts.

Nevertheless, privacy and data protection are not identical rights. On the one hand, data protection seems to fall in this aspect of privacy that is known, as seen above, as control over personal information. However, 'what privacy protects is irreducible to personal information'.[143] Privacy is a much broader concept that embodies a range of rights and values, such as non-interference or the right to be let alone, limited access to oneself, intimacy, seclusion, personhood, and so on according to the various definitions.[144]

On the other hand, not all personal data are necessarily 'private'. As the Court of First Instance (CFI) (now: General Court) rightly observed in *Bavarian Lager*:[145]

> It should be emphasised that the fact that the concept of 'private life' is a broad one, in accordance with the case-law of the European Court of Human Rights, and that the right to the protection of personal data may constitute one of the aspects of the right to respect for private life, *does not mean that all personal data necessarily fall within the concept of 'private life'*. A fortiori, *not all personal data are by their nature capable of undermining the private life of the person concerned.*[146]

This was confirmed by the Court of Justice that stated categorically in *Client Earth* that 'the concepts of "personal data"… and of "data relating to private life" are not to be confused.'[147] A different approach is very problematic, as the UK case *Durant v Financial Services Authority*[148] demonstrates. This case concerned an individual's request to access certain files containing information about some litigation he had with his bank. The Court of Appeal rejected his request on the basis that such information did not constitute personal data because personal data is only information which is

> biographical in a significant sense; has to have the individual as its focus; and has to affect an individual's privacy whether in his personal family life, business or professional activity.[149]

So restrictive a view of personal data cannot be accepted. Personal data is information relating to an identified or identifiable individual, and not information that

[142] Simitis comments: 'Privacy is an old and venerable subject.' Simitis, n 50 above, p 730.

[143] Rouvroy and Poullet, n 30 above, p 70.

[144] C Kuner, 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 *Computer Law and Security Review* 307, 309.

[145] Case T-194/04 *Bavarian Lager* (CFI, 8 November 2007).

[146] ibid, paras 118–19. Emphasis added.

[147] See Case C-615/13 P *Client Earth* (CJEU, 16 July 2015), para 32.

[148] *Durant v FSA* [2003] EWCA Civ 1746, Court of Appeal (Civil Division). For a comment see among others L Edwards, 'Taking the "Personal" Out of Personal Data: Durant v FSA and Its Impact on the Legal Regulation of CCTV' (2004) 1 *SCRIPT-ED* 341, 341.

[149] ibid. See also M Viola de Azevedo Cunha et al, 'Peer-to-Peer Privacy Violations and ISP Liability: Privacy Violations in the User-Generated Web' (2012) 2 *International Data Privacy Law* 50.

might affect 'in a significant sense' an individual's private life. This means that data protection and privacy are not exactly the same rights.[150]

Furthermore, unlike privacy's elusive and subjective nature, that makes this right different across different contexts and jurisdictions, data protection does not display any subjective elements in determining its limits and the grounds for remedies.[151] On the contrary, it has in many respects a procedural nature that makes it more 'objective' as a right.[152] Finally, data protection transcends informational privacy itself because, as is demonstrated in the section below, it serves other, further fundamental rights and values besides privacy.[153]

D. The Foundational Values of Data Protection

i. Privacy

It should be accepted that privacy is 'one—if not the—major'[154] value that data protection laws aim to safeguard.[155] Article 1 of both Convention No 108 and the Data Protection Directive states that their purpose is the protection of the fundamental rights and freedoms of the individual and in particular his right to *privacy*, with respect to the processing of personal data. Other international data protection instruments, such as the UN and the OECD Guidelines, also stress the link between data protection and privacy, but remain unclear about the exact nature of this link.[156] Moreover, national data protection texts, or their *travaux préparatoires,* often refer to privacy as one of the main aims[157] of their data protection legislation.[158] Privacy is, however, not defined in those data protection laws and, therefore, its meaning must be further sought 'partly in the substance of the principles laid down in the laws themselves, partly in the way those principles have been applied, and partly in general, societal notions of what privacy is'.[159] The fact that

[150] G González Fuster, n 33 above, p 271.

[151] R Polcak, 'Aims, Methods and Achievements in European Data Protection' (2009) 23 *International Review of Law Computers and Technology* 179, 181.

[152] See Bennett and Raab, n 11 above, p 8.

[153] S Gutwirth and M Hilderbrandt, 'Some Caveats on Profiling' in S Gutwirth, Y Roullet and PD Hert (eds), *Data Protection in a Profiled World* (Dordrecht, Springer, 2010) 31, 36; UK Information Commissioner, 'The Legal Framework: An Analysis of the "Constitutional" European Approach to Issues of data protection law', Study Project, 6.

[154] Bygrave, n 32 above, p 125.

[155] EJ Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York Law Review* 962, 1003; Fried, n 60 above, pp 477–78; Reiman, n 59 above, p 26; Westin, n 61 above, p 39.

[156] UK Information Commissioner, n 153 above, p 4.

[157] Writing on national data protection rules in Europe, Hondius contends that 'Privacy plays a certain role in all the laws, but never a dominating one.' See FW Hondius, 'Data Law in Europe' (1980) 16 *Stanford Journal of International Law* 87, 94–95.

[158] ibid, pp 92–93; Bygrave, n 32 above, p 116.

[159] L Bygrave, 'The Place of Privacy in Data Protection Law' (2001) 24 *University of New South Wales Law Journa*l 277, 278.

for a considerable time the subject-matter of an extensive legal framework before and after its inclusion in the Charter.

In fact, as mentioned above, the Explanations to the Charter refer to the Data Protection Directive as one of the sources of inspiration of this fundamental right.[257] Moreover, Article 52(7) EUCFR states that the explanations drawn up as a way of providing guidance in the interpretation of the Charter must be given 'due regard by the courts of the Union and of the Member States'. This raises pertinent questions regarding the relationship of the fundamental right to data protection with secondary legislation. These concern the content and the interpretation of this right. Besides the six constitutive principles of data protection expressly listed in paragraphs 2 and 3 of Article 8 EUCFR, can the content of the right to data protection be ascertained also with reference to secondary EU legislation? And, what if secondary legislation changes over time the level of protection offered? Would amendments resulting from subsequent secondary law affect the interpretation of Article 8 EUCFR?[258]

C. Reconstructing Data Protection: The Conditions

If the right to data protection is to be a bona fide fundamental right with a value of its own, it needs to be reconstructed, in order to satisfy three conditions. The first is that it should be recognised that the fundamental right to data protection has an 'autonomous content' of its own, which is independent from secondary legislation. The second condition that data protection needs to satisfy in order to be a fully-functional fundamental right is that it should be balanced against opposing rights or other interests as such, not through the proxy of privacy. The third condition is that data protection as a fundamental right should be able to function both positively and negatively. It should be able, on the one hand, to regulate, channel and control power, and on the other hand, to prohibit power.

i. The Fundamental Right to Data Protection Should Have an 'Autonomous' Content

Data protection may well have been regulated in a number of secondary law instruments in the EU legal order, but its inclusion in the Charter has a normative significance, only if this is disassociated from secondary legislation and it is recognised that as a fundamental right it has an 'autonomous' content of its own. This fundamental requirement derives from EU constitutional law and in particular,

for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L119/89.

[257] See above.

[258] The Austrian Supreme Court referred this question to the CJEU in the *Digital Rights Ireland* case.

Article 6(1) TEU, which stipulates that the rights, freedoms and principles set out in the EU Charter of Fundamental Rights have the same legal value as the Treaties. Since data protection is listed as a fundamental right in the Charter, the content of Article 8 EUCFR cannot be dependent on secondary legislation. In fact, the validity of secondary legislation, including secondary data protection laws and their subsequent amendments, should be reviewable in the light of the fundamental rights enshrined in the Charter, such as the fundamental right to data protection. Indeed, the CJEU in its seminal judgment in *Digital Rights Ireland*, reviewed (and annulled) the Data Retention Directive, which was listed as modification of secondary data protection legislation on the basis of Article 8 EUCFR.

It is accepted that there are some difficulties disassociating the fundamental right to data protection from relevant secondary legislation because certain concepts crucial for the right to the data protection, such as 'personal data' and 'processing' are defined in secondary legislation. This, however, does not mean that data protection as a fundamental right cannot have an 'autonomous' content. Such autonomous content does not require that the definition of these concepts should be necessarily different from the one provided in secondary legislation. It requires merely that this should be *independent* from secondary law. A similar argument can be made regarding the data protection principles listed in Article 8 EUCFR. The autonomous nature of the fundamental right to data protection does not prohibit the interpretation of these to draw inspiration from a broader list of data protection principles found in other international or European legal instruments. Indeed, this is confirmed by Article 52(7) EUCFR, which states that the Explanations of the Charter can provide guidance in its interpretation and should be given due regard by the courts of the Union and of the Member States.[259] The Explanations of the Charter refer to the Data Protection Directive and Convention No 108, and these could be taken into consideration when assessing and interpreting the data protection principles listed in Article 8 EUCFR. Nevertheless, the content of these principles remains autonomous and does not depend on secondary legislation. Thus, changes to the level of protection of personal data in subsequent amendments of secondary legislation do not affect the autonomous concept of the fundamental right to data protection enshrined in the Charter and are subject to review in the light of this.

Before turning to the second condition, it is necessary at this point to make a clarification about the content of the fundamental right to data protection. In particular, it should be considered what exactly constitutes this right, on the basis of which we should be able to assess any interferences with this. Article 8 EUCFR consists of three paragraphs: the first states that 'everyone has the right to the protection of personal data concerning him or her'; the second provides that such data must be processed fairly for specified purposes on a legitimate basis laid down by law and guarantees a right of access to the data and a right to rectification;

[259] See also Art 6(1) TEU.

the third paragraph makes compliance with these rules subject to control by an independent authority. In this respect, is the right to data protection enshrined in Article 8 (1) EUCFR or is it found in Article 8 EUCFR taken as a whole? The answer to this question is important because it will determine how an interference to this fundamental right is to be established. If we consider that the fundamental right to data protection is found in Article 8(1) solely, which stipulates that everyone has a right to the protection of his personal data, then any processing of such data will necessarily mean that it interferes with this fundamental right. If, on the other hand, we accept that the right is not confined only in the first paragraph of Article 8 but it is enshrined in all the three paragraphs of this Article, an interference with this will be established only when the processing in question interferes with one or more data protection principles. The case law of the CJEU has so far followed the former approach.[260] Nevertheless, I submit that the latter approach that sees the right to data protection in all the three paragraphs of Article 8 EUCFR is more correct and should, therefore, be adopted. This is for two reasons. First, the view that any type of processing of personal data interferes with the right to data protection, besides introducing a cyclical argument, is counter-intuitive because it also includes lawful processing that complies with all the requirements of Article 8 EUCFR. Secondly and more importantly, determining with accuracy the actual interference of a certain type of processing with the right to data protection is fundamental in order to be able to undertake a robust analysis of the permissibility of such interference on the basis of Article 52(1) EUCFR. Instead of merely assessing that the measure in question entails processing of personal data and, therefore, interferes with the right to data protection in general, it is important to determine the specific data protection principles the processing at issue interferes with. This makes the scope of the analysis clearer from the start and allows for a solid further examination of the justifiability of the established interference.

ii. A Balancing Mechanism for Data Protection

Data protection—as privacy—is not an absolute right.[261] On the contrary, it should be weighed against contrasting values and rights in a democratic society.[262] This means, furthermore, that data protection can legitimately be subjected to restrictions. These restrictions, however, will be permissible, insofar as they meet the following conditions: i) they are provided by law, ii) they pursue objectives

[260] For a detailed analysis see Chs 2, 3 and 6.

[261] The Court of Justice has repeatedly held that 'the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society'. See Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *v Land Hessen* (ECJ (GC), 9 November 2010), para 48 and Case C-543/09 *Deutsche Telekom* (ECJ, 5 May 2011), para 51. See also GDPR, Recital 4.

[262] As the Court of Justice has held, human rights are 'far from constituting unfettered prerogatives' and they are subject 'to limitations laid down in accordance with the public interest.' See Case 4/73 *Nold v Commission* [1974] ECR 491, para 14.

of general interest recognised by the Union or the need to protect the rights and freedoms of others, iii) they are necessary, iv) they conform with the principle of proportionality, and v) they respect the 'essence' of the right to data protection.[263]

This is the second condition that data protection needs to satisfy in order to be a fully functional fundamental right. It should be balanced against opposing interests as such, not through the proxy of privacy. This means that infringements of the right to data protection should be determined on the basis of the data protection principles themselves, with the application of the principle of proportionality,[264] without the need to recourse to the right to privacy. The processing, thus, of personal data should be deemed proportionate or disproportionate, on the basis of the specific fair information principle or principles, with which it interferes. Determining disproportionate processing on the basis of the right to privacy and not of the specific data protection principle that this goes against, is not only an unnecessary circumvention of the existing law that renders data protection virtually useless. It is also dangerous, because there could be instances of disproportionate processing of personal data that hardly, however, constitute disproportionate interferences with the right to privacy. The problem posed in the US Supreme Court case of *United States v Miller*[265] could be a useful example here. In this case, federal law enforcement officials issued subpoenas to two banks to produce a customer's financial records. The banks complied with the subpoenas, but the customer was not notified of the disclosure of the records until later in the course of prosecution. He argued that the subpoenas violated his Fourth Amendment rights,[266] but the Court concluded that he lacked a reasonable expectation of privacy in the financial records maintained by his bank,[267] because 'the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.'[268] According to the Court, '[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.'[269] Leaving aside the problems of the US constitutional protection of privacy through the 'legitimate expectations' doctrine, this example is also illuminating in the EU fundamental rights context.[270] The further use by the government of personal financial data is specifically

[263] Art 52 (1) EUCFR.

[264] On the relationship between the 'principle of proportionality' and the 'essential core' doctrine see the very interesting analysis of R Schutze, 'Three "Bills of Rights" for the European Union' (2011) 30 *Yearbook of European Law* 131, 140. See also R Alexy, *A Theory of Constitutional Rights* (Oxford, Oxford University Press, 2009) 51; L Zucca, *Constitutional Dilemmas: Conflicts of Fundamental Legal Rights in Europe and the USA* (Oxford, Oxford University Press, 2008).

[265] *United States v Miller* 425 US 435, 437 (1976).

[266] ibid, 438.

[267] ibid, 442.

[268] ibid, 443.

[269] ibid, 442.

[270] For a discussion on how the ECtHR has applied a 'reasonable expectations' test, see T Gómez-Arostegui, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35 *California Western International Law Journal* 153.

addressed by the purpose/use limitation principle, a keystone principle of data protection laws. It is not so evident, however, whether an interference with the right to privacy can be established here, without recourse to other fundamental rights and principles, such as, for instance, procedural rights of the individual to know if his personal information is further disseminated, or in certain cases, the principle of non-discrimination. Moreover, any potential claim of the customer against his bank would have to be established not on the basis of his right to privacy, but on breach of contractual obligations.

Taking data protection principles seriously is, therefore, a necessity. Data protection principles should not be seen as mere proclamations, void of any coercive meaning. Viewing fair information principles as coercive principles is not merely a theoretical issue emanating of the debate on the added value of data protection. It can have serious practical consequences in the drafting of legislation. This is because data protection principles are more specific and they can provide for prescriptive guidance better than the general privacy concept. They can be, thus, very informative for legislators, when they seek to adopt measures that clearly go against specific fair information principles. In these cases, stricter scrutiny against the test of proportionality should be applied, on the basis not only of privacy, but also of the specific data protection principle at stake. The problem remains the same, when the measure should be judged *ex post*, by courts: if a certain data protection principle is at issue, then it would be clearer if the court focused on that in order to perform the proportionality analysis, instead of seeking recourse to a general notion of privacy.

iii. The Essence of the Right to Data Protection: 'Hard Core' Data Protection Principles

In order for data protection to be able to function both positively and negatively, I argue that it should be recognised that this has an essential core that cannot be submitted to further restrictions. This follows from Article 52(1) EUCFR, that provides that 'any limitation of the exercise of the rights and freedoms recognized by this Charter must … respect the essence of those rights and freedoms.' This provision, which draws inspiration from national constitutions' pronouncements[271] and the ECtHR case law,[272] aims to guarantee that no limitation will deprive the rights and freedoms of the Charter of their substance.[273] Along the same lines, the ECJ has consistently held that restrictions to fundamental rights are justified when they 'do not constitute disproportionate and intolerable interference, impairing *the very substance* of the rights guaranteed'.[274] However, the Court has not clarified

[271] For instance, Art 19(2) of the German Basic Law provides that '[i]n no case may the essence of a basic right be affected.'

[272] *See Sporrong and Lönnroth v Sweden* (1982) Series A no 52, paras 58 and 60.

[273] Lenaerts, n 119 above, p 391.

[274] This pronouncement is often used with regard to the right to property. See Case 44/79 *Hauer* [1979] ECR 3727, para 23; Case 265/87 *Schräder HS Kraftfutter* [1989] ECR 2237, para 15; Case

whether the essence of a fundamental right refers to some kind of common and universal core of this right or whether this has a different meaning dependent on the circumstances of each particular case.[275]

Determining what constitutes the essence of the right to data protection is not an easy task. The Court referred to the essence of the right to data protection[276] in its judgment in *Digital Rights Ireland,*[277] asserting that this had not been adversely affected in that case because the Data Retention Directive contained certain principles of data protection and data security.[278] This pronouncement indeed confirms that the CJEU has recognised that data protection is a fully fledged fundamental right that operates both positively and negatively, and has an inviolable core. However, it is concerning that 'certain data protection and data security principles' may dangerously confine the essence of the fundamental right to data protection only to 'minimum safeguards'.

It should be noted, at the outset, that the essence of fundamental rights is necessarily a vague notion and should to an extent remain so. As is seen in detail below, the CJEU in *Digital Rights Ireland* and *Schrems* pinpointed in a dangerously accurate manner the essence of the right to privacy to the access to content of communications as opposed to metadata. Such an approach opened up criticisms concerning the artificiality of this division, but in my view, it is also risky because it ends up prescribing in definitive terms the essence of privacy. I disagree with such a prescriptive definition and, therefore, my attempt to approach the essence of data protection, is based on the premise that this should remain to an extent vague. Nevertheless, a number of points could be advanced here. The starting point for determining the essence of the right to data protection should be, of course, Article 8 of the Charter and the six data protection principles contained therein (the fair processing principle, the purpose specification principle, legitimate basis for processing, rights of access and rectification and the independent supervision principle). The fair processing principle includes further concerns and principles that should be considered even if not expressly listed in Article 8 EUCFR. Furthermore, there are certain types of processing that go against several, *cumulative* data protection principles. For instance, sensitive data should be shielded from certain categories of processing that can lead to profiling, especially if such processing is undertaken for different purposes from the ones that the data were initially collected for. Such processing that goes against a number of different data protection principles could be seen as an *aggravated* interference with the

C-293/97 *Standley and Others* [1999] ECR I-2603, para 54; Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* [2008] ECR I-6351, para 355; and, C-380/08 *ERG* [2010] ECR I-2007, para 80 (emphasis added).

[275] See Dirk Ehlers et al (eds), *European Fundamental Rights and Freedoms* (Berlin, De Gruyter, 2007) 393.

[276] The Court also discussed the essence of the right to privacy. See Case C-362/13 *Maximillian Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 39.

[277] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger* [2014] ECR I-238, para 40.

[278] ibid.

fundamental right to data protection. The purpose specification and limitation principle should also have a 'hard core', which should prohibit the secondary use of personal data, even if those are not necessarily sensitive. This 'essence' of the purpose limitation principle should apply when the further processing of personal data threatens the principle of non-discrimination or the core of the right to 'informational self-determination' of the individual. In essence, the 'hard core' of data protection would be what needs to be protected, so that the final values that data protection pursues such as dignity, informational self-determination and individual autonomy are safeguarded. This might require a recognition that the essence of one or more data protection principles has been touched upon in certain particular instances of processing.

7

Conclusions

I. THE FUNDAMENTAL RIGHT TO DATA PROTECTION RECONSTRUCTED

THE FIRST CHAPTER of this book examined the normative added value of the fundamental right to data protection in the EU legal order. It explored the current theories about this right and concluded that three important limitations that this has faced since its emergence in the EU constitutional order impair it from functioning as a fully fledged fundamental right with a normative value of its own: its *interconnectivity* with privacy, its *linking* with secondary legislation, and the *elusiveness* of its content.

The first limitation arises from its relationship with the right to privacy. Privacy and data protection have been inextricably intertwined for several reasons: their scope overlaps to the extent that they both refer to the concept of 'control over personal information', privacy is an aim that data protection pursues and the two rights have been frequently associated in legislative instruments. For instance, Article 1(1) of the Data Protection Directive provides that Member States must 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.' This interconnectivity between the two rights has prompted some scholars[1] to argue that data protection operates as a transparency tool that permits certain processing, while privacy as the opacity tool, against which permissible limitations should be judged. In its initial case law following the entry into force of the Lisbon Treaty that made the EU Charter of Fundamental Rights binding, the CJEU considered that the two rights could not be dissociated, and were to be seen together as 'the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter'.[2] This association of the two rights prevents the right to data protection from having a normative significance on its own, since all permissible limitations are reviewed either on the basis of the right to privacy or through the combination of this right to the seemingly insufficient data protection.

[1] P De Hert and S Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in Erik Claes et al (eds), *Privacy and the Criminal Law* (Antwerpen, Intersentia, 2006) 61.

[2] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *v Land Hessen* (CJEU (GC), 9 November 2010), para 52.

The second limitation that data protection faces in its operation as a fully fledged fundamental right concerns its relationship with secondary legislation. Data protection was regulated in different secondary EU law instruments long before its elevation to the status of a fundamental right. Data protection legislation has been subject to review and amendment by the EU institutions, and the recent adoption of the General Data Protection Regulation and the Data Protection Directive are significant instruments for the modernisation of this legislation in order to be able to respond to the challenges that arise from new technologies, the Internet and the modern techniques of processing Big Data. However, if the fundamental right to data protection enshrined in Article 8 EUCFR is made dependent on secondary legislation to the extent that its content has to be assessed on the basis of this, this right cannot have a normative value. Such linking is all the more dangerous, because subsequent amendments of secondary data protection legislation affecting the standard of protection offered may have an impact on the fundamental right to data protection.

Thirdly, data protection is limited from operating as a fully fledged fundamental right because of the uncertainty that surrounds the actual content of this right. Two pertinent questions arise in this respect: first, is the right to data protection confined in paragraph 1 of Article 8 EUCFR, which contains the general recognition that 'everyone has the right to the protection of personal data concerning him or her', or should all the three paragraphs of this article be taken into account in order to establish an interference with this right? Secondly, is the content of the fundamental right to data protection determined only by the six elements explicitly included in paragraphs 2 and 3 of Article 8 EUCFR (principle of fair processing, purpose specification principle, legitimate basis laid down by the law, right to access, right to rectification and independent supervision), or can it be argued that further data protection principles not expressly mentioned in this article can be part of this right?

This book developed a theory on data protection that reconstructed this fundamental right on the basis of three conditions. The first condition requires that the fundamental right to data protection has an 'autonomous content' of its own, which is independent from secondary legislation. The second condition provides that data protection should be balanced against opposing rights or other interests as such, not through the proxy of privacy. The third condition stipulates that data protection as a fundamental right should be able to function both positively and negatively, in that it should be able to both regulate and prohibit power.

The first condition, which requires that the fundamental right to data protection has an 'autonomous content' of its own, arises from the supremacy of the Charter and the rights enshrined therein in the hierarchy of EU norms. The fundamental right to data protection is autonomous of secondary data protection legislation, and this legislation and its subsequent amendments are reviewable on the basis of this right. However, it was clarified that such autonomous content does not bar courts from drawing inspiration from secondary legislative instruments

to assist them with the interpretation of technical concepts such as 'personal data' or 'processing' or the meaning of different data protection principles enshrined in Article 8 EUCFR, in accordance with the relevant provision of Article 52(7) EUCFR, which points to the Explanations of the Charter that mention the Data Protection Directive. In this regard, I argue that the content of the fundamental right to data protection is not necessarily confined to the six principles expressly listed in Article 8 EUCFR; further fair information principles inspired from various sources of national, international and supranational law can be part of Article 8 EUCFR. This is consistent with the fact that the article itself stipulates the principle of fair processing, which incorporates further data protection requirements, such as transparency and accountability of processing. Such an interpretation was confirmed by the CJEU in *Digital Rights Ireland*,[3] where the Court held that data security, a principle which is not expressly mentioned in Article 8 EUCFR, indeed forms part of this fundamental right. What should be cautioned, however, is that the content of the fundamental right to data protection should be autonomous, and, thus, independent from secondary law. The book also argued that the right to data protection is to be found in Article 8 EUCFR taken as a whole, reading together paragraphs 1, 2 and 3 of this Article, and not only on the basis of paragraph 1. If the right is to be found in the whole Article 8 EUCFR, this means that processing of personal data in accordance with paragraphs 2 and 3 does not constitute an interference with this fundamental right. It is only counter-intuitive to consider that any processing of personal data interferes with the fundamental right to data protection and as the data surveillance case studies have shown, this also presents an extremely superficial and even erroneous analysis.

The second condition that data protection has to satisfy in order to operate as a fundamental right with a value of its own requires that this should be balanced against opposing rights or other interests as such, not through the proxy of privacy. Any potential interference with the right to data protection should be determined on the basis of the data protection principles themselves, with the application of the principle of proportionality, without the need to recourse to the right to privacy. Determining disproportionate processing on the basis of the right to privacy, and not of the specific data protection principle that this goes against, is not only an unnecessary circumvention of the existing EU constitutional law that renders the right to data protection virtually useless, but it is also erroneous and dangerous, because there could be instances of disproportionate processing of personal data that hardly constitute disproportionate interferences with the right to privacy. Such an approach, furthermore, accepts that an interference with data protection does not necessarily imply an interference with privacy and vice-versa

[3] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2014] ECR I-238.

and, thus, avoids the fallacies committed by Advocate General Cruz Villalón in his Opinion in *Digital Rights Ireland*.[4] The two rights are autonomous to each other and should operate in this way.

The third condition requires that data protection as a fundamental right should be able to function both positively and negatively. This requires recognition that data protection has an essential core that cannot be submitted to further restrictions, in accordance with Article 52(1) EUCFR. By recognising that data protection has an essential core, this right is able to prohibit power as well as regulate it—it can, therefore, perform the function of a fundamental right with an intrinsic normative value. Determining what constitutes the essence of the right to data protection is not an easy task. Recent case law has provided some guidance, but the issue still remains—rightly—vague. The Court spoke of the essence of the right to data protection in *Digital Rights Ireland*,[5] connecting it to 'certain principles of data protection and data security'. In this respect, it should be cautioned that the essence of the fundamental right to data protection—or any fundamental right—should not operate as a 'floor',[6] offering merely minimum standards of protection. The essence of data protection would be what needs to be protected, so that the final values that this right pursues, and in particular dignity, are safeguarded. The essence of this right should play a role when an 'aggravated' interference based on processing that goes against a multitude of data protection principles occurs. It was explained that, for instance, the processing of data of the whole population, carried out for different purposes from those for which the data were initially collected, for a long period of time, and that can lead to profiling and discrimination based on 'predetermined criteria and scenarios'[7] developed by algorithms, could touch on the essence of the fundamental right to data protection, since it interferes *cumulatively* with different data protection principles, and challenges the dignity of individuals.

Thus reconstructed to satisfy these three conditions, there is no reason why data protection cannot operate as a *bona fide* fundamental right and have a normative significance. Before this right is examined in the context of data surveillance, it is worth summarising the Court's case law on the right to data protection as this emerged in Chapter 2. Before the constitutional entrenchment of data protection as a fundamental right in the Charter, the Court in *Österreichischer Rundfunk*[8] and *Lindqvist*[9] dissociated the application of EU data protection legislation from internal market objectives. Since the entry into force of the Lisbon Treaty, its

[4] Opinion of AG Cruz Villalón in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, delivered on 12 September 2013.

[5] *Digital Rights Ireland*, n 3 above, para 40.

[6] See F Fabbrini, *Fundamental Rights in Europe—Challenges and Transformations in Comparative Perspective* (Oxford, Oxford University Press, 2014) 37.

[7] Opinion of AG Mengozzi in Opinion 1/15, delivered on 8 September 2016, para 261.

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

[9] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

case law on the fundamental right to data protection has evolved progressively, with the analysis identifying three stages of maturity. At the first stage, the Court could not dissociate data protection from privacy, and assessed the permissibility of limitations on what I call the '*Schecke* formula' of viewing the two rights together. In this respect, the Court felt compelled to often repeat in its case law the close connection between data protection and privacy. At the second stage, the Court started to slowly distinguish between the two rights, but it did so in a somewhat confusing way, struggling with the relevant terminology. At the third stage, the case law of the CJEU not only proves that the Court can now see the two rights separately, but it also demonstrates how the permissible limitations to these rights should be assessed. Although the Court is, therefore, to be praised for reaching maturity in its case law concerning the right to data protection, some questions regarding the content and essence of this right have been left unanswered. These concern mainly the Court's insistence to read the fundamental right to data protection only in paragraph 1 of Article 8 EUCFR and to consider, therefore, that any processing of personal data constitutes an interference with this right.

II. DATA SURVEILLANCE AND THE FUNDAMENTAL RIGHT TO DATA PROTECTION

The analysis of the four case studies on communications metadata (Chapter 3), travel data (Chapter 4), financial data (Chapter 5) and Internet data (Chapter 6) surveillance in Part II of the book reveals a number of common trends as to the *why*, the *how* and the *what for* of data surveillance. Data surveillance measures, whatever their focus, have *similar purposes*; are made possible through the (compelled) *cooperation of private actors*; they collect a significant *volume* of data; that are further processed and analysed in a *probabilistic* manner.

As emerged from all the cases discussed, fighting terrorism is one of the main purposes of surveillance. Some measures had further purposes, such as the fight against serious crime (Data Retention Directive), the prevention of transnational crime (PNR) and the acquisition of foreign intelligence (PRISM and UPSTREAM surveillance). Furthermore, data surveillance is undertaken through the cooperation of private actors that collect the data in the first place. Electronic communications' metadata retention was based on the collection of such information by communications service providers; PNR data are collected by airline companies; financial data are extracted from the SWIFT database that provides financial messaging services; and information on Internet communications and activities has been obtained by the US authorities from leading Internet companies. In all the four case of data surveillance examined, the personal data are granted to the private actors by individuals for completely unrelated purposes, such as billing purposes (metadata retention); in order to book a flight (PNR); to transfer money (TFTP); and to use the services provided by Internet companies, such as Facebook and Google (PRISM). The volume of data collected and targeted under

the four examined surveillance cases is extensive. They all concern a generalised, mass retention of the electronic communications and Internet communications of virtually every individual that uses the respective services of communications providers, airlines and SWIFT. This retention is often not based on evidence of suspicion, but is undertaken pre-emptively in a probabilistic manner to uncover 'risky' individuals on the basis of algorithm processing and analysis of 'terrorist patterns'.

Data surveillance poses serious challenges to the fundamental rights to privacy and data protection. These should be approached by assessing the potential interference with the two rights separately, as the Court rightly did in *Digital Rights Ireland*. Metadata retention, such as that prescribed in the Data Retention Directive, the TFTP and Internet surveillance programmes, such as PRISM and UPSTREAM collection interfere with the confidentiality of electronic and financial communications and, therefore, the right to privacy. It was argued that PNR is a different story, since most of the data retained in this case, albeit personal, are hardly private. Nevertheless, it was submitted that all the four data surveillance programmes examined in Part II interfere with the fundamental right to data protection as this was reconstructed in Chapter 1. The section below brings together the conclusions drawn from the substantive analysis of the four case studies and explains the steps that should be taken in order to assess the permissibility of the interference with this fundamental right.

III. COUNTER-TERRORISM DATA SURVEILLANCE AND PERMISSIBLE LIMITATIONS TO THE FUNDAMENTAL RIGHT TO DATA PROTECTION

The analysis of permissible limitations should follow Article 52(1) EUCFR, which provides that any limitation of a right of the Charter should be provided for by law; meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; be necessary; be subject to the principle of proportionality; and respect the essence of the right. Before I turn to these conditions, an initial comment should be made about the CJEU's approach to data protection. Taking into account the importance of fighting terrorism, the Court should be praised for not following a 'reductionist' approach[10] to data protection (and privacy) through the adoption of strict standing conditions, that require some degree of 'harm' to allow the challenging of data surveillance measures. In addition, the CJEU has adopted a strict standard of judicial review of surveillance considering the seriousness of the interference this poses to data protection and privacy.

First, it must be established that data surveillance programmes pose an interference to the fundamental right to data protection. The mere processing of

[10] See L Floridi, 'The ontological interpretation of informational privacy' (2005) 7 *Ethics and Information Technology* 185, 194.

personal data is not enough to establish such an interference. All three paragraphs of Article 8 EUCFR should be taken into account and processing that does not comply with them, because it goes against certain fair information principles should be considered to interfere with Article 8 EUCFR. The fair information principles interfered with should be mentioned expressly in the analysis in order for this to be able to proceed to assess their permissibility. It was concluded from the four surveillance cases analysed that these interfere with the purpose limitation principle, the data minimisation principle, the data security principle, in many cases the data are retained for longer periods than necessary, many measures do not provide for adequate due process rights for data subjects or these rights—if provided—are substantially watered down in the protection they offer, and finally some of these measures do not guarantee control by an independent supervisory authority, thus failing to comply with the requirements laid down by the CJEU in *Commission v Hungary*.[11]

Having established that there is an interference with the fundamental right to data protection, it should be examined whether this is 'provided for by law'. In this respect, the measure must be foreseeable and accessible to individuals who should also be made aware of the potential access of public authorities to the data they grant to private actors in order to receive a service, such as to book a flight or transfer money or send an e-mail or a text message or browse the Internet. Surveillance programmes that have operated secretly for years and were revealed by media articles or whistle-blowers, such as TFTP and PRISM, do not satisfy this requirement.

Fighting terrorism and crime are considered objectives of general interest recognised by the Union and, therefore, there are a few difficulties for data surveillance measures to meet this requirement. It should be noted, however, that indiscriminate, mass data surveillance should not be undertaken for purposes such as border control management, as it was seen in the EU–US PNR case.

Assessing the necessity of a data surveillance measure requires an examination of the appropriateness of such a measure, its effectiveness to fight terrorism and an assessment whether this is the least restrictive measure that could be adopted in order to attain this objective. The data surveillance case studies examined were considered in general appropriate to fight terrorism. However, their effectiveness is far from proven, as robust empirical evidence as to their efficacy is not available. This is highly problematic, given that data surveillance is extremely broad in its scope and targets the whole population without providing for any exception for individuals that do not have any link to terrorism or serious crime. The broad reach of metadata surveillance as well as the fact that the Data Retention Directive did not determine the conditions of access to the data and did not make the retention period subject to any differentiation depending on the usefulness of the data retained were considered to violate the necessity requirement in *Digital Rights*

[11] Case C-288/12 *Commission v Hungary* (CJEU (GC), 8 April 2014).

Ireland. Data surveillance measures should include robust provisions guaranteeing data security, the irreversible destruction of the data at the end of the data retention period and control by an independent authority. Even so, it is argued that data surveillance as such interferes disproportionately with the purpose limitation principle. Indeed, using data that individuals provided to private actors for totally unrelated commercial purposes empties this principle of its very content. The fact that the data surveillance measures provide the legal basis for the purpose deviation does not change this conclusion. It is crucial, therefore, that the courts and in particular the CJEU address this issue and decide whether the purpose limitation principle still has a meaning in the era of Big Data surveillance. Finally, data surveillance as a whole should be examined under the scope of proportionality *stricto sensu* to assess its advantages and the risks it engenders in a democratic society.[12]

Finally, data surveillance measures cannot compromise the essence of the fundamental right to data protection. The CJEU has demonstrated in *Schrems* that essence of fundamental rights does not only have a symbolic value, but this can indeed play a decisive role on the invalidation of a data surveillance measure on the basis of its incompatibility with the fundamental rights at stake. What constitutes the essence of the right to data protection, however, is still unclear and vague. While this is not *per se* problematic, this book argued that the essence of this right cannot be confined to a 'floor' concept of safeguarding of certain minimum data protection and data security safeguards, as *Digital Rights Ireland* suggested. Such an approach would imply that Article 8 EUCFR can function only as a transparency tool that channels power, and not as a fully fledged fundamental right that can prohibit power.

IV. THE NORMATIVE VALUE OF THE FUNDAMENTAL RIGHT TO DATA PROTECTION IN COUNTER-TERRORISM SURVEILLANCE

Having discussed the different case studies, we should go back to the core question of this book: does data protection have a normative added value as a fundamental right? First, it should be observed that the fundamental right to data protection is neither obsolete next to privacy, nor does it serve as the *lex specialis* of privacy. The scope of the two rights may overlap to an extent, but it is different, as the PNR case demonstrated. Moreover, data protection pursues multifarious values that go beyond privacy. But even if data surveillance raises both privacy and data protection issues, as was seen in the context of metadata, financial and Internet data surveillance, the fundamental right to data protection does not lose its added value. The two rights can co-exist and operate independently next to each other

[12] See Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*, delivered on 19 July 2016, para 262.

to provide the individual with the most effective protective framework against counter-terrorism surveillance. The fundamental right to data protection does not threaten privacy and there is no hierarchy between the two rights.

The value of data protection is not limited to the fact that it indeed adds something to privacy, as the PNR case showed. The fundamental right to data protection has a *legal* and *practical* significance of its own. In legal terms, data protection is instrumental in ensuring informational self-determination, autonomy, non-discrimination and ultimately human dignity. Furthermore, as reconstructed in Chapter 1, data protection can stand as a bulwark against counter-terrorism data surveillance and the probabilistic processing of personal data. But data protection also has a *practical* significance. The right's *procedural nature* expressed through the various information principles makes its demands clearly articulated for legislators, law enforcement and intelligence authorities, private actors whose compelled assistance is crucial for the carrying out of data surveillance, individuals and courts. The fair information principles provide specific guidance on the permissibility of processing and in this respect they should be used by legislators when they lay down counter-terrorism legislation. Law enforcement and intelligence authorities can use these principles as guidance when they conduct surveillance activities. Private actors are also bound by the fundamental right to data protection and have certain obligations as 'processors' of personal data. The constitutional entrenchment of data protection as a fundamental right in the EU has made this right more visible to the data subjects that often feel powerless in front of the modern means of surveillance. Finally, the reconstructed fundamental right to data protection is valuable for courts that are called upon to assess *ex post* the compliance of surveillance measures in the light of this fundamental right.

The discussion contained in this book would be incomplete if it did not concern itself with the question of whether counter-terrorism data surveillance can be—at all—compatible with fundamental rights. All the data surveillance measures examined in this book were found to interfere seriously with the fundamental rights to privacy and data protection. The only way that data surveillance can be made compatible with fundamental rights in order to pursue the legitimate objective of fighting terrorism is through its compliance with different data protection principles and requirements. These demand that:

— personal data are collected and processed on the basis of objective reasons that justify their usefulness in fighting terrorism, and the mass, indiscriminate collection of data of all the people without any differentiation just because they are readily available is not acceptable (data minimisation principle);
— there are measures in place ensuring data security and the protection of information from unauthorised access (data security principle);
— the conditions of access and use of personal data are clearly defined on the basis of objective criteria;

— data subjects have the right to know about the potential further purposes of the processing of their personal data and they can exercise effectively their rights to access, rectification and erasure as well as having avenues of effective judicial redress; and
— the processing of the personal data collected and, in particular, its use by counter-terrorism authorities is subject to independent control.

Data protection principles, therefore, are the only way forward for the compatibility of data surveillance with fundamental rights. The challenge for legislators is now to design such measures that respect the fundamental rights to privacy and data protection and do not deprive them of their very essence. Regulating data surveillance on the basis of the fundamental right to data protection and its fair information principles would be a first step towards this direction. But the reconstructed right to data protection does not only serve in regulating permissible data surveillance; it can altogether prohibit this if it compromises its ultimate values.

This book has studied the value of the right to data protection in the most difficult context: counter-terrorism data surveillance. The study of other instances of processing is work left for the future; nevertheless, it is hoped that the reader will have obtained important insights about this right's capabilities that are transferrable to further different contexts of processing.