Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right

Maria Tzanou*

Abstract

- Data protection has always been linked to privacy in such a way that it is very difficult to assess its very notion, its purpose, and its value without falling back to privacy.
- The entry into force of the Lisbon Treaty on 1 December 2009 marked a historic moment for data protection: the right was elevated to the status of a fundamental right within the EU legal order, alongside the right to privacy.
- This article discusses the shortcomings of the current theories and the existing case law of the ECJ on data protection and argues that data protection should be 'reconstructed' in order to operate as a fully-fledged fundamental right next to the right to privacy.
- Two conditions are necessary for this: First, a 'core' or 'essence' of the right to data protection should be recognized. Second, infringements of the right to data protection should be determined solely on the basis of the relevant data protection principles themselves without the need to recourse to the right to privacy.

Introduction

Athena, the goddess of wisdom, and patron of Athens, sprang, according to ancient Greek mythology, fully armed and brandishing a sharp javelin out of her father's, Zeus's, head, after he was tortured by a terrible headache. The life of privacy and data protection is reminiscent of this beautiful ancient Greek myth. The two rights seem to share a parent–child relationship. Data protection appeared as an offspring of privacy and the two rights still seem inextricably tied up together with a birth cord. However—as does any child—data protection is trying to mark its own way in life.

At the outset, the two rights are mudded into a confusing cluster of differences and similarities. Books and articles on privacy normally begin with the assertion that this is the most difficult right to define.[1] On the other hand, legal scholars writing on data protection do not seem to find it hard to describe the main essence of data protection laws: they are rules that 'specifically regulate all or more stages in the processing'[2] of *personal* information; which is normally defined as any information relating to an identified or identifiable person.[3]

Be that as it may, the conceptual difficulty of defining privacy 'does not undermine its importance'.[4] Privacy has been described as 'the right most valued by civilized men'[5] and its value has rarely been questioned. On the other hand, there is a general confusion among courts and legal scholars about the benefits of a right to data protection and doubts have been raised concerning its entrenchment.[6] 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,

* Lecturer in Law, Department of Law and Criminology, Edge Hill University, UK. E-mail: Maria.Tzanou@edgehill.ac.uk. I am much obliged to Professor Valsamis Mitsilegas, Professor Tuomas Ojanen, Professor Giovanni Sartor and my PhD thesis supervisor at the EUI Professor Martin Scheinin for their valuable input on my PhD thesis and this article. I would also like to thank the anonymous reviewer for the valuable comments provided. All opinions as well as mistakes naturally remain my own.

1 William Beaney, 'The Right to Privacy and American Law' (1966) 31 Law & Contemporary Problems 253, 255; C Kuner and others, 'Privacy-an elusive concept' (2011) 1 International Data Privacy Law 141.

2 Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International: The Hague/London/New York 2002) 2.

3 Article 2 (a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281 of 23.11.1995, p. 31.

4 Adam Moore, *Privacy Rights: Moral and Legal Foundations* (Pennsylvania State University Press: University Park, PA, 2010) 11; Hilary Delany and Eoin Carolan, *The Right to Privacy: A Doctrinal and Comparative Analysis* (Thomson Round Hall: Dublin, 2008) 4.

5 *Olmstead v United States*, 277 U.S. 438, 478 (1928) (Brandeis. J. dissenting). See also Daniel Solove, *Understanding Privacy* (Harvard University Press: Cambridge, MA, 2008) 3.

6 Lucas 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 & Security Report 31.

does it add anything to the right to privacy, however the latter is being defined? Despite these doubts, and characterized by what Stefano Rodotà has called a 'veritable social, political, and institutional schizophrenia',[7] data protection was elevated to the status of a fundamental right alongside the right to privacy.[8]

Scholars, however, tend to agree that privacy and data protection share a common characteristic: they are both confronted by serious interference in the contemporary information society.[9]

The present contribution focuses on the infant of the two rights: the right to personal data protection. A large body of law already pertains to data protection, however there are numerous uncertainties concerning the capabilities of the right to personal data protection to resolve problems and provide for an effective protection. This paper endeavours to set forth a theory of data protection that will reshape in a clear and comprehensive manner the understanding of this right. It attempts to bring clarity to the concept of data protection and its underlying values and aims. It discusses the current theories and the existing case law on data protection by identifying their shortcomings. Finally, it elaborates a new theory on data protection and addresses its benefits and possible limitations.

Conceptualizing 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.'[10] The EU Data Protection Directive (DPD) sees 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'.[11]

The notions of 'processing' and of 'personal data', thus appear central for the understanding of the concept of data protection. In general terms, 'processing' can be seen as any operation performed upon the data, from their collection, recording, storage, use, to their disclosure, dissemination, erasure, and destruction. The data are considered personal when they can be linked to a certain individual.

Data protection can thus be understood as referring to this set of legal rules that aims to protect the rights, freedoms, and interests of individuals, whose personal data are collected, stored, processed, disseminated, destroyed, etc.[12] The ultimate objective is to ensure 'fairness in the processing of data and, to some extent, fairness in the outcomes of such processing'.[13] The fairness of processing is safeguarded by a number of principles (also known as 'fair information principles' or 'data protection principles'), such as: collection and purpose limitation, data quality, data security, openness and transparency of processing, accountability, and individual participation principle.

Data protection as 'informational self-determination'

Understanding data protection, however, as management of personal information is not enough. Data protection is not simply about informational privacy; it is about informational *autonomy.*[14] This concept of data protection cannot find a more accurate description in legal terms than in the right to 'informational self-determination' ('informationelle Selbstbestimmung'), as pronounced by the German Constitutional Court (*Bundesverfassungsgericht*) in its landmark Census decision ('Volkszählungsurteil').[15] According to the Court, the right to 'informational self-determination' guarantees, in principle, the power of the individual to determine for himself the disclosure and use of his data. The right is based on Articles 1 (1) (human dignity) and 2 (1) (personality right) of the German Constitution. These require 'clearly defined conditions of processing', which ensure 'that under the conditions of automatic collection and processing of personal data the individual is not reduced to a mere object of information'.[16]

The German Constitutional Court, in its decision, couched its concerns regarding modern methods of data processing that can result in treating individuals as objects. The technical means of storing information,

7 Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer: Dordrecht, 2009) 77.

8 Article 8 of the Charter of Fundamental Rights of the European Union [2010] OJ C83/389.

9 David Lyon, *Surveillance after September 11* (Polity Press in association with Blackwell Pub. Inc.: Cambridge/Malden, MA, 2003); David H. Flaherty, 'On the Utility of Constitutional Rights to Privacy and Data Protection' [1990] Case Western Reserve Law Review 831, 835–6; Michael Froomkin, 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461.

10 Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer: Dordrecht, 2009) 3.

11 Article 1 (1).

12 Frits Hondius, *Emerging Data Protection in Europe* (North-Holland Pub. Co.; American Elsevier Pub. Co.: Amsterdam; New York 1975) 1.

13 Bygrave (n 2), at 168.

14 Emphasis added.

15 Volkszählungsurteil, 65 BVerfGE 1, 68–69 (1983).

16 Ibid.

the automatic data processing, and the combination of data in integrated information systems add up to a partial or virtually complete personality profile ('Persönlichkeitsbild'), whose truth and application the person concerned has no sufficient means to control. The right to informational self-determination precludes a social order in which citizens can no longer know who knows what, when, and on what occasion about them, as such would not only impair their chances of development, 'but it would also impair the common good, because self-determination is an elementary functional condition of a free democratic community'.[17]

Dancing together apart: Privacy and data protection

Much ink has been spilt recently, after the constitutional entrenchment at the EU level of a right to data protection, on the exact nature of the relationship between privacy and data protection. The debate, a lively one among European scholars, is concerned with the question of whether data protection can be conceived as a 'separate',[18] or 'autonomous' fundamental right, 'distinct'[19] from the right to privacy, or whether it should be regarded as a mere aspect of privacy. I do not wish to enter this discussion by focusing on terms such as the 'separateness' or the 'distinction' between the two rights, the more neutral assertion that privacy and data protection 'interact in a variety of ways'[20] is more preferable here. That being said, a number of points should be made clear on this issue.

First, we cannot lose sight of the EU constitutional reality: data protection has been enshrined 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 context at least, data protection is considered (or expected) to add something to privacy.

Second, we cannot lose sight of the historical reality: data protection legislation is a relative newcomer; it only appeared on the scene in the 1970s as a response to concerns raised about the increasingly centralized processing of personal data and the establishment of huge data banks.[21] The first piece of data protection legislation was enacted in 1970 by the German state of Hesse.[22] It was followed by Sweden in 1973[23] and, subsequently, by other European countries. In most cases, legislators chose to legitimize data protection regulation by simply referring to traditional privacy concepts.[24] On the other hand, to rephrase Spiros Simitis, privacy is 'an old and venerable'[25] 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 into the aspect of privacy that is known as control over personal information.[26] However, 'what privacy protects is irreducible to personal information'.[27] Privacy is a much broader concept that embodies a range of rights and values, such as the right to be let alone, intimacy, seclusion, personhood, and so on according to the various definitions.[28] On the other hand, as the Court of First Instance (CFI) (now the General Court) rightly observed in *Bavarian Lager*, not all personal data are necessarily private: 'not all personal data are by their nature capable of undermining the private life of the person concerned'.[29] Furthermore, unlike privacy's elusive and subjective nature that makes the right different in different contexts and jurisdictions, data protection has an essential *procedural* nature that it makes it more objective as a right in different contexts.[30] Finally, data protection is more than informational privacy itself because, as will be demonstrated below, it serves other, further fundamental rights and values besides privacy.[31]

17 Ibid.

18 Nicolas Scandamis, Frantzis Sigalas, and Sofoklis Stratakis, 'Rival Freedoms in terms of Security: The Case of Data Protection and the Criterion of Connexity' (CEPS, CHALLENGE December 2007) Research Paper No. 7 15.

19 Gloria González Fuster, Paul de Hert and Serge Gutwirth, 'The Law-Security Nexus in Europe: State-of the-art report' Deliverable submitted November 2008 (M8) in fulfillment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the International Security Continuum in Europe (INEX) WP2 D2.1, 11.

20 Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer: Dordrecht, 2009) 45.

21 Bygrave (n 2), at 93.

22 Datenschutzgesetz, 7 Oct. 1970, § 6, 1 Gesetz- und Verordnungsblatt für das Land Hessen 625 (1970).

23 Datalagen (Swedish Data Act) of May 11, 1973, entered into force 1 July 1973.

24 Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review 707, 709.

25 Ibid, at 707.

26 On privacy as control over personal information see Alan Westin, *Privacy and Freedom* (Bodley Head: London, 1970) 31.

27 Rouvroy and Poullet (n 20), at 70.

28 Christopher Kuner, 'An international legal framework for data protection: Issues and prospects' (2009) 25 Computer Law & Security Review 307, 309.

29 Case T-194/04 *Bavarian Lager*, judgment of the Court of First Instance of 8 November 2007, paras 118–119.

30 See Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge, MA, 2006) 8.

31 Serge Gutwirth and Mireille Hilderbrandt, 'Some Caveats on Profiling' in Serge Gutwirth and others (eds), *Data Protection in a Profiled World* (Springer: Dordrecht, 2010) 36.

Underlying values behind data protection

That privacy is 'one—if not *the*—major'[32] value that data protection laws aim to safeguard is not questioned. A look at the first article of both the Convention No. 108 of the Council of Europe[33] and the EU Data Protection Directive[34] confirms this. Other international data protection instruments, such as the UN and the OECD Guidelines, also stress the link between data protection and privacy, but remain, however 'rather *unclear* about the precise nature of this link'.[35] Moreover, national data protection texts or their *travaux préparatoires* refer to the right to privacy as one of the main aims of their data protection legislation.[36] Paradoxically enough, though, privacy is 'never directly defined in those data protection laws that employ the term', and therefore its 'meaning for the purposes of data protection law must be 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'.[37]

Privacy may well be the main value behind data protection rules, but data protection legislation advances further interests. A set of interests that data protection laws aim to safeguard, further to privacy, concerns the security of the information systems ('data security') and the quality of data contained therein ('data quality'). 'Data security' pertains to keeping the data secure against certain risks, such as being lost or accessed by unauthorized persons. In this regard, the EU Data Protection Directive requires data controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. The measures should ensure a level of security appropriate to the risks represented by the processing and the nature of the data.[38] Furthermore, the Directive obliges data controllers to choose a processor that provides sufficient guarantees of technical and organizational security with respect to data processing.[39]

'Data quality' refers to the accuracy, adequacy, relevance, and up-to-dateness of the personal information.[40] Personal information that is accurate, adequate, and up-to-date safeguards, first of all, the interests of data controllers because it allows them to make accurate decisions based on valid, adequate and relevant data. Equally, it is in the interests of the data subjects, as inaccurate information held on them means concomitant inaccuracy in the sketching of the 'digital persona' of those individuals.

The processing of personal data bears inherent imbalances. These are manifest in the asymmetries between the two main actors of information processing: the data subject, on the one hand, and data controllers on the other hand. Data subjects are facing a situation where '(a) there is virtually no limit to the amount of Information that can be recorded, (b) there is virtually no limit to the scope of analysis that can be done—bounded only by human ingenuity, and (c) the information may be stored virtually forever.'[41]

Data protection rules attempt to address this problem[42] by embodying the values of transparency, foreseeability in data processing, accountability of data controllers, and—to the extent that is possible—participation of the data subject in the processing of his/her information.[43] These values are voiced in a number of fair information principles; above all, in the principle of fair and lawful processing, in the purpose specification principle, and in the individual participation principle.

There is a further value safeguarded by data protection rules that goes beyond the above categories of interests: the principle of non-discrimination. This principle is particularly pertinent for data protection regulations that aim to grapple with certain processes, such as 'profiling', which can be discriminatory. The concern of data protection legislation for the principle of non-discrimination is, above all, manifest in the rules that require the additional protection of the processing of special categories of data that are normally

32 Bygrave (n 2), at 125.

33 Article 1 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), adopted at 28.1.1981, entered into force 1 Oct. 1985.

34 Article 1 (1) DPD.

35 UK Information Commissioner, 'The Legal Framework: An analysis of the "constitutional" European approach to issues of data protection law', February 2004, Study Project 4.

36 See Frits W. Hondius, 'Data Law in Europe' (1980) 16 Stan J Int'l L 87, 94–5.

37 Lee Bygrave, 'The Place of Privacy in Data Protection Law' (2001) 24 University of New South Wales Law Journal 277, 278.

38 Article 17 (1).

39 Article 17 (2).

40 Article 6 (1) (c) and (d).

41 Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559, 576.

42 See Herbert Burkert, 'Towards a New Generation of Data Protection Legislation' in Gutwirth and others (eds), *Reinventing Data Protection?* (Springer: Dordrecht, 2009) 339.

43 See C Kuner and others 'The challenge of "big data" for data protection' (2012) 2 International Data Privacy Law 47–49.

described as 'sensitive'. Personal data that reveal racial or ethnic origin, political opinions, religious beliefs, sexual orientation, and health, are subject to enhanced protection, and their processing is, in principle, prohibited as a default rule in the European data protection context.[44] This is because the processing of such data can lead to illegal discrimination. Concerns about discriminatory processes are also manifest in provisions, such as Article 15 DPD, aimed at protecting individuals against fully automated decision making.

Finally, while it might be wrong to regard the proportionality principle as an autonomous value pursued by data protection laws, proportionality concerns run through data protection legislation and they underpin the operation of most of the fair information principles.[45] Direct references to the principle of proportionality can be found in the rules that require that personal data should be 'relevant' and 'not excessive' in relation to the purposes for which they are collected and further processed; that they are 'necessary'; and, that they are kept for no longer than is necessary for the purposes for which the data were collected or further processed.[46]

Theories of data protection and their shortcomings

Despite extensive writing by scholars and practitioners on various data protection issues, the research could pinpoint two theories on the nature of data protection which will be approached critically in this section alongside a discussion of the relevant case law of the European Court of Justice (ECJ) (now the Court of Justice of the EU), before I turn to the submission of a new theory on data protection.

Until now, the most comprehensive theory on data protection has been developed by Paul de Hert and Serge Gutwirth.[47] Their theory discusses the respective roles that privacy and data protection can play in a democratic constitutional State. It is based on the premise that privacy and data protection can be seen as two distinct legal tools of power control that perform different, but complementary, functions (an approach I call the 'separatist model'). According to the two authors, 'much can . . . be learned from making and ascertaining the *difference* in scope, rationale and logic between privacy on the one hand, and data protection on the other'.[48] In this respect, privacy is conceived as a tool of *opacity*, while data protection is seen as a tool of *transparency*. Their function is different: opacity tools 'embody normative choices about the limits of power'; transparency tools 'come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power'.[49] Privacy, hence, on the one hand, as a tool of opacity, aims to protect individuals against the illegitimate and excessive use of power (non-interference); data protection, on the other hand, as a tool of transparency, is directed towards the control and channelling of legitimate use of power. Pursuant to this approach, while data protection can be seen as offering a regulated acceptance, privacy presents a prohibition rule, which is, however, in general subject to exceptions, since privacy is not an absolute right itself.[50] In terms of 'how much of which tool is necessary when?', de Hert and Gutwirth explain that data protection transparency tools, should be considered as the default rules; 'only in rare cases or after due consideration of actual risks will prohibitive opacity measures be taken to protect rights and freedoms and to promote trust in the Information Society'.[51]

It cannot be denied that the 'separatist model' has many obvious merits. It attempts to understand and ascertain the role of data protection in a democratic society through the very content of its principles: they are designed to promote procedural justice, rather than normative (or substantive) justice. Therefore, according to de Hert and Gutwirth, data protection does not operate in a prohibitive manner, but it 'ruptures' the common legal logic: it replaces the traditional prohibitionary rule 'thou shall not kill' with 'thou can process personal data under certain circumstances'.[52] The prohibitive role is found by these authors in the function of privacy. Due to these different functions, de Hert and Gutwirth explain, for the first time, why data protection is needed alongside with privacy in a democratic constitutional state. Its added value can be seen, according to these authors, in the clear separation of the two rights, which implies a distinction between the

44 Article 8 (1).

45 Lee Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer: Dordrecht, 2009); CB Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) 1 International Data Privacy Law 239–48.

46 Article 6 (1) (c), (d) and (e).

47 Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes and others (eds), *Privacy and the Criminal Law* (Intersentia 2006).

48 Ibid, 62.

49 Ibid, 70

50 Ibid, 94

51 Ibid, 96.

52 Ibid, 77.

legal tools of opacity, on the one hand, and transparency, on the other.

There is, however, a fundamental problem with de Hert's and Gutwirth's approach that undermines the basic core of their argument altogether. The theory of these two authors seeks to establish, above all, the added value of the constitutional entrenchment of a separate right to data protection, next to the right to privacy. The enthusiasm of the two scholars could not be more evident: 'Apparently, something new is happening at constitutional level';[53] 'very recently, the proper role of data protection has received constitutional recognition in Article 8 of the 2000 Charter of Fundamental Rights of the EU';[54] 'this recognition of a constitutional right should be welcomed',[55] and so on. There is, however, a paradox in their line of thinking: their theory, while it aims to be a theory on data protection, does not focus on data protection itself. Rather, the added value of data protection is demonstrated through its distinction from privacy. By preaching separation, they strive to show the indispensability of data protection. But, their very argument proves them wrong. In the end, according to de Hert and Gutwirth, everything will be judged on the basis of privacy, as the tool of opacity[56] will be the benchmark for establishing prohibited interference. Data protection, as a transparency tool, merely describes the permitted level of processing; the limits will then be set on the basis of privacy. This, however, means that data protection is not indispensable: we could live well without it. Of course we are better off with it, as it has some utility as a useful transparency tool, but still we could live without it, since every possible interference will be judged against privacy. De Hert and Gutwirth fail to prove, therefore, why data protection is so fundamental, that it explains its constitutional entrenchment.

Despite its problems, the 'separatist' approach is the most comprehensive theory of data protection elaborated so far. The research could identify in the literature a further approach to data protection, with the essential caveat, however, that this has been developed mainly as a critical response to the 'separatist' model analysed above, and thus, cannot be viewed as a standalone, comprehensive theory on data protection.

Replying essentially to de Hert and Gutwirth, Antoinette Rouvroy and Yves Poullet argue that privacy and data protection have 'an "intermediate" rather than a "final" value, because they are "tools" through which more fundamental values, or more "basic" rights—namely human dignity and individual personality rights—are pursued'.[57] For this reason, they should be conceived as *instruments* for fostering the autonomic capabilities of individuals that are necessary for sustaining a lively democracy (an approach I call the 'instrumentalist' model). The two authors explain that the emergence of a right to data protection is due to the technological evolutions that 'may require legal protections of privacy to evolve, simply because those technological evolutions threaten, in new ways, the fundamental value of personal autonomy'.[58] They support this argument by invoking the German Constitutional Court's Census decision, according to which, 'the development of the data processing technologies obliged the State to revise and adapt the guarantees it provides to individuals in order to protect and foster the capabilities needed to implement their right to freely self-determine their personality'.[59]

Rouvroy and Poullet contend, however, that privacy and data protection 'are not to be put on the same footing',[60] because they are different tools for enabling individual reflexive autonomy. They criticize, therefore, the acknowledgement of the right to data protection as a fundamental right, distinct to the traditional fundamental right to privacy in the EUCFR, because

> by placing the right to data protection on the same level as privacy, the European text carries the risk that the fundamental anchoring of data protection regimes in the fundamental values of dignity and autonomy will soon be forgotten by lawyers and that legislators will soon forget to refer to these fundamental values in order to continuously assess data protection legislation taking into account the evolution of the Information Society.[61]

In this regard, they explain, in a rather confusing way, that making the right to data protection a distinct fundamental right

> risks obscuring the essential relation existing between privacy and data protection and further estrange data protection from the fundamental values of human dignity and individual autonomy, foundational to the concept of

53 De Hert and Gutwirth (n 10), at 7.
54 De Hert and Gutwirth (n 47), at 81.
55 Ibid.
56 Opacity as a notion for describing privacy is also problematic because it appears to conceive of privacy as secrecy.
57 Rouvroy and Poullet (n 20), at 53.
58 Ibid, 54
59 Ibid, 55.
60 Ibid, 70.
61 Ibid, 71.

> privacy in which data protection regimes have their roots.[62]

Besides the fact that the 'instrumentalist' approach fails to provide a robust analysis of the right to data protection, it is fraught with fears that remain unsubstantiated. It is not clear why data protection cannot have an instrumental value, while at the same time being on an equal footing with privacy. The two authors seem to negate any value of data protection, because this might allegedly end up in trumping the instrumental value of privacy, and thus undermine privacy as a fundamental right. Rouvroy and Poullet make a valid point about the uniqueness of the final goals of the two rights (be that autonomy or dignity or the right to individual personality), but, they do not convince why the constitutional entrenchment of data protection is so harmful.

Data protection in the case law of the European Court of Justice

Several judgments have been pronounced by the ECJ concerning data protection issues. Most often, they regard preliminary rulings on questions of interpretation of the Data Protection Directive. If we attempt a general comment on this case law, this would be that 'the Court, in essence, has interpreted an internal market harmonization instrument (the Directive) in a manner that fosters the protection of a fundamental right'.[63] This notwithstanding, the Court has been accused of viewing 'data protection as privacy, no more no less'.[64] According to this argument, the Court's approach is simple: 'A breach of the right to privacy implies an unlawful processing in the sense of the Directive; no breach of privacy implies no breach of the Directive.'[65] The analysis will discuss this argument by focusing on three cases where the Court of Justice dealt with the nature of data protection: *Österreichischer Rundfunk*,[66] *Promusicae*,[67] and *Schecke*.[68]

Österreichischer Rundfunk was a preliminary ruling case on the compatibility with Community law of an Austrian provision requiring entities which were subject to control by the Austrian Court of Audit, the Rechnungshof, to inform the latter about the salaries of their employees when they exceeded a certain level. This information was subsequently published by the Rechnungshof in a report which contained the names of the persons and the level of their respective salaries. In this respect, the Court was asked to rule whether the DPD was applicable at all to this control activity exercised by the Rechnungshof.

Having established that the applicability of the DPD is not based on the 'connection' of the processing activity with the internal market, on the substantive issue of the nature of data protection, the Court seems to think that this should be interpreted on the basis of the right to privacy:

> It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe *fundamental freedoms*, in particular the right to *privacy*, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures.[69]

This pronouncement seems to suggest that the Court, at the time of the decision, was only concerned over certain forms of processing that might infringe fundamental rights, and in particular the right to privacy; in this case, the protection afforded to fundamental rights as general principles of EU law would apply. Having stated this, the ECJ went on to examine in *Österreichischer Rundfunk* whether the activities of the Rechnungshof constituted interference with the right to privacy. It concluded that:

> while the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the Convention.[70]

This approach of the Court, albeit understandable, is problematic because by failing to recognize data protection as a fundamental right, all possible interferences

62 Ibid, 74.

63 Maria Tzanou, 'Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection' (2010) 6 Croatian Yearbook of European Law & Policy 53, 59.

64 De Hert and Gutwirth (n 10), at 33.

65 Ibid, 32.

66 Joined Cases C-465/00, C-138/01, and C-139/01, *Österreichischer Rundfunk*, Judgment of 20 May 2003, Full Court, [2003] ECR I-4989.

67 Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, judgment of 29 January 2008.

68 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*, Judgment of the Court (Grand Chamber) of 9 November 2010.

69 Joined Cases C-465/00, C-138/01, and C-139/01, *Österreichischer Rundfunk*, para. 68.

70 Ibid., para. 74.

have to be assessed on the basis of the right to privacy. Thus, activities that would constitute interferences with data protection, such as the recording of remuneration, are not deemed to interfere with the right to privacy unless the recorded data are communicated to third parties.

While the ECJ in *Österreichischer Rundfunk* focused solely on the DPD, in *Promusicae*, it recognized for the first time data protection as a fundamental right enshrined in the Charter. *Promusicae* concerned the refusal of a commercial company in Spain, which provides internet access services, Telefónica, to disclose to Promusicae—a non-profit-making organization of producers and publishers of musical and audiovisual recordings, acting on behalf of its members who were holders of intellectual property rights—the personal data of certain persons to whom it provided internet access services. Promusicae sought disclosure of the above information before the Commercial Court of Madrid in order to be able to bring civil proceedings against those persons, who, according to it, used the KaZaA file exchange program (peer-to-peer) and provided access in shared files of personal computers to phonograms in which the members of Promusicae held the exploitation rights. The Spanish Court referred the issue to the ECJ by asking it essentially whether Community law, in particular Directives 2000/31,[71] 2001/29,[72] and 2004/48,[73] read in the light of Articles 17 and 47 of the EUCFR, require member states to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.

Having established that the secondary Community legislation did not provide a clear answer on the issue at stake, the Court turned its attention to primary EU constitutional law, namely fundamental rights. In this part of its analysis, it noted from the outset that while the fundamental right to property, which includes intellectual property rights such as copyright, and the fundamental right to effective judicial protection constitute general principles of Community law,[74] the situation in respect of which the national court put the question at issue involves, in addition to those two rights, a *further fundamental* right, namely the right that 'guarantees protection of personal data and *hence of private life*'.[75] This is the first time that the Court expressly recognized that the right to data protection enjoys the status of a fundamental right within the EU. It did so by looking at Article 8 of the EUCFR—even though the Charter was not legally binding at that point—which expressly proclaims the right to data protection. It seems, though, that the ECJ in this case went one step forward from its existing case law concerning the Charter: until *Promusicae*, if a right was contained in the Charter, this created a presumption that it was protected under the general principles of Community law.[76] In *Promusicae*, however, the fact that the protection of personal data was enshrined in the Charter was enough for the ECJ to identify it as an autonomous fundamental right.[77]

Promusicae is interesting from this point of view; in terms of substance, however, it marked no real difference from the ECJ's understanding of data protection in *Österreichischer Rundfunk*. The Court seems to think that data protection is a fundamental right that guarantees the protection of personal data and *hence of private life*. The balancing of fundamental rights, therefore, in this case will take place between 'the right to respect for *private life* on the one hand and the rights to protection of property and to an effective remedy on the other'.[78] Data protection is not mentioned by the Court since, apparently, it is a part of privacy.

It was in *Schecke* that the Court for the first time had to judge the validity of EU law in the light of the provisions of the—by now—legally binding Charter.[79] In this case, the Court was presented with a unique opportunity to clarify its position regarding the nature of data protection as a fundamental right. The case concerned the questions raised in the course of proceedings between two German nationals, a natural and a legal person, and the Land Hessen concerning the publication on the Internet site of the Bundesanstalt für Landwirtschaft und Ernährung (Federal Office for Agri-

71 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1.

72 Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167/10.

73 Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157/32.

74 Case C-275/06 *Promusicae*, para. 62.

75 Ibid, para. 63 (emphasis added).

76 Michael Dougan, 'The Treaty of Lisbon 2007: Winning Minds, not Hearts' (2008) 45 Common Market Law Review 617, 662.

77 Maria Tzanou, 'Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence' in Christina Akrivopoulou and Athanasios Psygkas (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and practices* (Information Science Reference: Hershey, PA, 2011) 275.

78 Case C-275/06 *Promusicae*, para. 65 (emphasis added).

79 Sara Iglesias Sánchez, 'The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights' (2012) 49 Common Market Law Review 1565, 1581.

culture and Food) of personal data relating to them as recipients of funds from the European Agricultural Guarantee Fund (EAGF) or the European Agricultural Fund for Rural Development (EAFRD). The publication was mandatory pursuant to Article 44a of Regulation No 1290/2005,[80] which obliges member states to ensure annual *ex post* publication of the beneficiaries of the EAGF and the EAFRD and the amounts received per beneficiary under each of these Funds.

Before turning to the reasoning of the Court of Justice, it is worth taking a look at the national court's position. This opined that the obligation to publish under Article 44a of Regulation No 1290/2005 constituted an unjustified interference with the fundamental right to the protection of personal data.[81] In particular, it considered that that provision, which pursues the aim of increasing the transparency of the use of European funds, does not improve the prevention of irregularities, since extensive control mechanisms exist for that purpose. In any event, according to the German court, that obligation to publish was not proportionate to the aim pursued, because the Regulation did not limit access to the Internet site concerned to 'Internet Protocol' (IP) addresses situated in the European Union, and it was not possible to withdraw the data from the Internet after expiry of the two-year period laid down in Article 3(3) of Regulation No 259/2008.[82] The German court's pronouncement on the case is very important, because it essentially invited the ECJ to recognize data protection as a self-standing fundamental right: the court suggested that any possible interference had to be determined on the basis of the data protection principles without any recourse to privacy.

The ECJ, however, did not follow that path. It started by pointing out that the relevant provision on publication of the Regulation should be assessed in the light of the EU Charter of Fundamental Rights, which constituted, at the time of the delivery of the decision, binding EU law. The Court mentioned that Article 8 EUCFR was the relevant Charter provision at this case, but with the necessary clarification that 'that fundamental right is *closely connected* with the right to respect of private life expressed in Article 7 of the Charter'.[83] Having said that, the Court proceeded its analysis on the permissible limitations that can be imposed to the right to data protection by confounding, however, data protection and privacy, in what it called 'the right to respect for private life with regard to the processing of personal data, recognized by Articles 7 and 8 of the Charter'.[84]

Reconstructing data protection

Method: How should we approach data protection?

Despite the differences in the conclusions of the two theories on data protection analysed above—the 'separatist' is recognizing an added value to data protection; the 'instrumentalist' negating it—and the relevant case law of the ECJ, they all share a common insightful point: they both view data protection through privacy. They attempt, therefore, to formulate a data protection theory by looking into its relationship with privacy.

Starting from the premise that data protection is a fundamental right, at least within the EU legal framework, I argue that an approach to understanding the added value—if there be any—of this right must have a focus. Its focus should be data protection, not its possible interactions with privacy. This does not mean, however, that I deny that the two rights are closely related. Privacy is an umbrella notion for a plurality of things that covers aspects of data protection in any case. This does not imply, necessarily, that data protection has no added value. My argument, therefore, is that if we want to approach this value, we should try to see data protection in isolation for a moment.

Is data protection sufficiently 'mature' to stand alone? Problems and limitations

That being said, why is it that the two theoretical attempts to approach data protection and the ECJ in its decisions find it necessary to view data protection through the lens of privacy? Certainly, data protection pursues, above all, privacy objectives, but is this the real reason? Or is there something missing from data protection rules that makes the right unable to stand alone? De Hert and Gutwirth view data protection as a tool of transparency, aimed to channel or regulate, but not prohibit power.[85] Data protection operates,

80 Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, OJ L 209, p. 1.

81 Joined Cases C-92/09 and C-93/09 *Schecke*, para. 30.

82 Ibid, para. 31.

83 Ibid, para. 47 (emphasis added).

84 Ibid, para. 52.

85 Along the same lines, Hijmans and Scirocco argue that 'the right to data protection itself cannot be exercised without rules specifying the right. The right does not prohibit processing of personal data but basically formulates the conditions under which processing is legitimate'. Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?' (2009) 46 Common Market Law Review 1485, 1518.

therefore, only as an affirmative liberty. The same approach is adopted by the ECJ that finds it necessary to fall back on privacy and examine the two rights together in order to determine if certain forms of processing are illegitimate.

Indeed, taking a closer look at Article 8 of the EUCFR, one can agree that data protection is depicted in affirmative terms, as a transparency tool. The first paragraph of Article 8 introduces the general right—everyone has the right to the protection of personal data concerning him or her—while the second paragraph goes on to set the rules for permissible processing—fair processing, for specified purposes, on the basis of the consent of the person concerned or some other legitimate basis, granting the data subject the right of access and rectification. The right to privacy in Article 7 is also formulated in an affirmative way. One should not be confused though. Pursuant to Article 52 (3) EUCFR, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the Convention.[86] The right to privacy is found in Article 8 of the ECHR.[87] The second paragraph stipulates that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It is clear, therefore, that the right to privacy in the EUCFR has the function of the opacity, non-interference tool.

Viewing data protection merely in affirmative terms is, however, problematic. The problem is not only theoretical. As Cohen astutely points out, 'the conventional wisdom is that . . . affirmative liberty claims are weaker and less principled than negative liberty claims'.[88] This is why data protection cannot stand alone as a fundamental right. This is why the right to privacy is needed in the end to determine the prohibitive instances of non-interference.

I argue that the way in which data protection has been drafted obstructs the right itself to operate independently from privacy. Contrary to what de Hert and Gutwirth contend, the value of a fundamental right to data protection, as it stands now, is limited: it can operate only as a transparency tool, but illegitimate interferences will still be determined on the basis of privacy,[89] as the analysis of the relevant case law of the ECJ above has demonstrated. These limitations, whether they are attributed to the drafters of the right,[90] or the particularities of its genesis and its initial drafting to take into account economic concerns, demonstrate that data protection is not 'mature' enough, as it currently stands, to operate alone.

Reconstructing data protection: 'Hard core' data protection principles

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 certain conditions. The first 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 submit that this can be done, by recognizing a 'core' or 'essence' of the right to data protection that cannot be subjected to restrictions. Determining which elements of the fair information principles represent the 'essential core' of the right to data protection is not an easy task. The starting point should be, of course, the Charter. The core essence of the right to data protection is laid down in Article 8 (*fair* processing for *specified purposes*, *rights of access*, and *rectification*).[91] Furthermore, sensitive data, such as data revealing racial or ethnic origin, political and religious beliefs, health and sexual life, should be shielded from certain categories of processing, especially if this is undertaken for the use of the data for different purposes from the ones initially collected. The purpose specification principle should also have a 'hard core' which will prohibit the secondary use of personal data, even if those are not necessarily sensitive. This 'essence' of the purpose specification principle should apply when the further

86 The same Article clarifies, however, that 'this provision shall not prevent Union law providing more extensive protection'. See Koen Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375, 394.

87 The Explanations relating to the Charter confirm that 'Article 7 corresponds to Article 8 ECHR'. See the explanations relating to the Charter of Fundamental Rights, OJ [2007] C 303/17.

88 Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stan L Rev 1373, 1400; David Currie, 'Positive and Negative Constitutional Rights' (1986) 53 U Chicago L Rev. 864, 887.

89 Martin Scheinin and Mathias Vermeulen, 'DETECTER, Detection Technologies, Terrorism, Ethics and Human Rights', 2011European Commission, Seventh Framework Programme 7.

90 C Kuner and others, 'Let's not kill all the privacy laws (and lawyers)' (2011) 1 International Data Privacy Law 209.

91 Emphasis added.

processing of personal data threatens the principle of non-discrimination or the core substance 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 individual autonomy, dignity, and personal identity are safeguarded. Thus reconstructed, it is difficult to see why the right to data protection cannot stand independently on the side of the right to privacy.

A balancing mechanism for data protection

Data protection—as privacy—is not an absolute right. On the contrary, it should be weighed against contrasting values and rights in a democratic society. This means, furthermore, that data protection can be legitimately 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 a legitimate aim; (iii) they are necessary in a democratic society; (iv) they conform with the principle of proportionality; and (v) they respect the 'essence' of the right to data protection.

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, without the need to recourse to the right to privacy. The processing of personal data should, therefore, be deemed proportionate or disproportionate on the basis of the specific fair information principle 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, however, hardly constitute disproportionate interferences with the right to privacy.

The problem posed in the case *United States v Miller*[92] of the US Supreme Court 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 his records until later in the course of the prosecution. He argued that the subpoenas violated his Fourth Amendment rights, but the Court decided that he lacked a reasonable expectation of privacy in the financial records maintained by the banks because 'the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities'.[93] 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'.[94] Leaving aside the problems of the US constitutional protection of privacy through the 'legitimate expectations' doctrine, this example is also illuminating for the EU fundamental rights context. The further use by the government of personal financial data is specifically 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 a 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 from 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, in this way, very informative for legislators when they seek to adopt measures that clearly go against specific fair information principles. In these cases, stricter scrutiny should be applied, not only on the basis 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 a propor-

92 425 U.S. 435, 437 (1976).
93 Id. at 443.
94 Id. at 442.

tionality analysis, instead of seeking recourse to a general notion of privacy.[95]

As seen above, the ECJ has not adopted this approach so far, even if this is possible under the current constitutional developments in the EU. The Court prefers to see the two rights together as 'the right to respect for private life with regard to the processing of personal data'. Privacy is needed in the equation, because on the basis of this, the possible interferences will be determined, according to Article 8 (2) ECHR. In *Schecke*, the ECJ missed a chance to follow the way shown by the German court and recognize for the first time that data protection can operate independently. This reading could have been possible, though, since the Court could have applied directly to the right to data protection in Article 8 EUCFR the conditions of Article 52 (1) EUCFR, without the need to go through Article 52 (3) to the relevant provision of Article 8 (2) ECHR on the permissible limitations to the right to privacy. One cannot deny, however, that the ECJ's approach is understandable since the Charter became legally binding only very recently, and the case law by the Court on the EUCFR and, *a fortiori*, Article 8 including a separate provision on data protection is still sparse and in its 'formative years'. Moreover, the ECHR has traditionally enjoyed 'special relevance' within the EU legal order.

Conclusions

Data protection has always been linked to privacy in such a way that it is difficult to assess its very notion, its purpose, and its value without falling back to privacy. Despite this uneasiness, data protection has been elevated to the status of a fundamental right within the EU legal order, rising proudly next to the right to privacy. Its nature, however, continues to confuse literature and courts. Does it have an added value or is it all about privacy in the end?

Answering this question is not easy, especially taking into account how the right stands at the moment. It seems to be able to operate only positively, which makes it impossible to survive without privacy at its side. The present contribution argued that the EU Charter of Fundamental Rights provides European courts with all the necessary tools to reconstruct data protection to a fully-functional fundamental right that adds something to privacy. The time has come for data protection to operate as a real fundamental right: both positively and negatively. Data protection should be able not only to regulate, but also to prohibit, power. This means that infringements of the right to data protection should be determined solely on the basis of the relevant data protection principles themselves, with the application of the principle of proportionality, without the need to recourse to the right to privacy.

Until now, with the Lisbon Treaty counting three years of life, this path has not been taken up by the ECJ. It is crucial, however, that the Court of Justice reconsiders its approach to data protection if this is ever to mark its own way as an independent fundamental right within the EU or is always to live in the shadow of privacy.

doi:10.1093/idpl/ipt004
Advance Access Publication 20 March 2013

95 As Hijmans and Scirocco point out, 'presently the test of proportionality of limitations of the right to data protection is already carried out, based on Article 8 ECHR'. Hijmans and Scirocco (n 85), at 1518. However, recent case-law shows that the ECJ performs proportionality analysis. See for instance, *Schecke*, para. 72 where the Court notes that 'it is . . . necessary to ascertain whether the limitation imposed on the rights conferred by Articles 7 and 8 of the Charter is proportionate to the legitimate aim pursued'.