To be published in :
Daniel Guagnin, Leon Hempel, Carla Ilten, Carla, Inga Kroener, Daniel Neyland, Hector Postigo, Eds , *Managing Privacy Through Accountability*. 2012. Palgrave Macmillan

Beyond accountability, the return to privacy?[1]

Raphaël Gellert & Serge Gutwirth

1. Introduction: Privacy and data protection, a matter of confusion

1.1 Different conceptions of privacy

There is great confusion as to what the exact meaning of privacy is.
As Solove puts it, privacy is a concept in disarray. It is a sweeping concept and nobody can articulate what it means.[2]

In this respect,[3] privacy has successively been conceptualised in terms of "right to be let alone",[4] control over personal information,[5] the construction of one's identity,[6] informational self-determination,[7] or contextual integrity.[8]

What clearly emerges from these attempted conceptualisations of privacy is that privacy is a multidimensional, multifaceted concept, the complexity of which is therefore hard to grasp within a single conceptual setting. Some do argue that privacy should not be defined at all, since such definition would bear the risk of limiting and 'freezing' its meaning and effects (especially in the legal field).[9]

---

[1] This contribution is based on the first deliverable of the EU FP7 PRESCIENT project, to which the VUB is participating. See, http://www.prescient-project.eu/prescient/index.php
[2] Solove, D., J., *Understanding Privacy*, London, Cambridge, MA: Harvard University Press, 2008, p. 1.
[3] The following list of conceptualisations is not exhaustive. For a very comprehensive taxonomy, see, Solove, D., J., 2008, *op. cit.*, chapter 2; Nissenbaum, H., *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford: Stanford Law Books, 2010.
[4] Warren, S., D., Brandeis, L.,D., "The Right to Privacy", *Harvard Law Review*, vol. 4, n° 193, 1890, pp. 193-220.
[5] Westin, A., *Privacy and Freedom*, New-York: Atheneum, 1967.
[6] Agre, Ph., E., Rotenberg, M., *Technology and Privacy: The New Landscape*, Cambridge, MA: MIT Press, 1997. More specifically, these authors define privacy as "the freedom from unreasonable constraints on constructing identity and control over aspects of identity projected to the world", *op. cit.*, p. 7.
[7] Rouvroy, A., Poullet, Y., "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", *in* Gutwirth, S., Poullet, Y., De Hert, P., de Terwagne, C., and Nouwt, S., (eds.), *Reinventing Data Protection?*, Dordrecht: Springer, 2009, pp. 45-76.
[8] Nissenbaum, H., "Privacy as Contextual Integrity", Washington Law Review, vol. 79, 2004, pp. 119-158; Nissenbaum, 2008, op. cit., Part II.
[9] Gutwirth, S., *Privacy in the information age*, Lanham: Rowman & Littlefield, 2002.

Indeed, as Solove points out, some theories are too narrow (solely focusing on information, or access to the self), others are too broad (e.g., the right to be let alone, which is an emanation of personhood), whereas others are both too broad and too narrow at times.[10]
However, beyond these controversies, it is not contested that privacy can operate within two different social settings. The first, relates to conceptions of privacy as seclusion and concerns situations wherein a given individual lives free from the attention of others, not being watched. The second concerns individuals in a social or public context, i.e., an individual evolving among his peers or as an actor in the public sphere. In such a situation, more informational versions of privacy might come into play as social interactions necessarily entail that third parties will be in possession of information concerning the individual (one could argue that social interactions are information *per se*, as the latter have no choice but to recourse to semiotic mediation). It follows from this that obviously many aspects of an individual's life are captured in data or "information".[11] This is the more true in contemporary societies, which many have referred to as "surveillance societies", given that governments process so much data on citizens on a daily basis. But it is also true of corporations (though, not necessarily for the same reasons).

It follows from this, that in the contemporary societal context, concepts of privacy as informational control have increasingly come to the fore.

1.2 Data protection legislations

Within this context, governments have strived to protect the (informational) privacy of its citizens through data protection legislations. This is the reason why the rationale of all data protection legislation is, *inter alia*, to protect the privacy of individuals.[12]
In Europe (but also elsewhere), an impressive armada of data protection legislation has been adopted. In this respect, the oldest instruments are the OECD "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" from 1980.[13] These guidelines however (as well as the other ensuing documents adopted within this framework), are not binding. The first binding international legal instrument with regard to data protection is Convention 108 of 1981 of the Council of Europe.[14] The principles contained therein are still of relevance, and have also served as a basis for the ensuing European Directives. Indeed, due to its wide range (its scope is not limited like that of the data protection directive, and it is open to third states), it

[10] Solove, D., J., 2008, op. cit., pp. 37-38.
[11] Roosendaal, A., *We are all connected to Facebook... By Facebook!*, on file with the author, 2011, p. 17.
[12] See, e.g., article 1.1 of Directive 95/46/EC. The rationales behind data protection legislation are of course numerous and complex. Apart, the protection of citizens' privacy, important economic interests related to the free flow of personal data are at stake, and some authors have raised the question whether data protection legislation is "*little more than a privacy-friendly front hiding the true purpose of promoting an economic policy which puts personal data on the same level as any other economic product*", *in* Gutwirth, S., *Privacy and the Information Age*, Lanham: Rowman & Littlefield, 2002, p. 89.
[13] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. See also, Wright D., De Hert P. & Gutwirth S., "Are the OECD Guidelines at 30 showing their age?", *Communications of the ACM*, Vol. 54/2, February 2011, 119-127.
[14] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108, Strasbourg, 18 January 1981.

is therefore still considered as a standard in data protection legislation.[15]

At EU level, several directives have been adopted. The most important piece of regulation is EU 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, commonly known as the Data Protection Directive.[16]

Other relevant EU instruments include the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters of 27 November 2008[17], the 2002/58/EC Directive (E-Privacy Directive) which actualises the data protection principles to face some of the new challenges raised by continuing developments in the electronic communications sector[18] and Regulation EC No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[19] In addition, the Treaty of Lisbon on the Functioning of the European Union (TFEU) features a general constitutional provision on data protection (art. 16),[20] and gave the EU Charter of Fundamental Rights (EUCFR) a binding character in the EU.

Equally, in the policy/academic discourse, many talk about the protection of citizens' privacy in the context of data protection legislations.[21] Such a focus on data protection legislation has led to a shift whereby the protection of privacy started to be only thought of in terms of data protection legislation, even though there exists a legal right to privacy that is enshrined in the European Convention of Human Rights (ECHR), and in most or many European Constitutions.

This shift, we contend, is not without dangers because it tends to overlook the right to

---

[15] See, Gutwirth, S., *Privacy and the Information Age*, Lanham: Rowman & Littlefield, 2002; De Hert, P., and Bellanova, R., *Data Protection in the Area of Freedom, Security and Justice: A System Still to Be Fully Developed?*, Brussels: European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2009, p. 7.

[16] European Parliament and the Council, Directive 95/46/EC 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 L 281, 23.11.1995. This directive is currently under revision. See, http://ec.europa.eu/justice/policies/privacy/review/index_en.htm.

[17] Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008. This Framework Decision aimed to fill the gap left by the restricted scope of the Data Protection Directive, by providing a regulatory framework for the protection of personal data in the area of police and judicial co-operation, or what was called the "third pillar" before the entry into force of the Lisbon Treaty.

[18] Recital 4 mentions that the aim of the directive is to translate "the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector".

[19] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1, 12.01.2001.

[20] "Everyone has the right to the protection of their personal data" (art.16[1] TFEU).

[21] For example, data protection legislation has been blamed for having "too often accepted exceptions to privacy on less than satisfactory grounds", Guild, E., Carrera, S., "The European Union's Area of Freedom, Security and Justice Ten Years On", *in* Guild, E., Carrera, S., Eggenschwiler, A., (eds), *The European Union's Area of Freedom, Security and Justice Ten Years On - Successes and future challenges under the Stockholm Programme*, Brussels, European Union and Centre for European Policy Studies**,** 2010, pp. 1-12.

privacy, which is different from the right to data protection, although they are very much interrelated. Ultimately, this disinterest in the right to privacy and its correlative narrowing focus on data protection can be seen as a possible explanation as to why the protection offered by the right to data protection is far from being flawless.

Yet, in the face of the ever-growing challenges that ICTs are posing to the privacy of individuals, the emphasis continues to be solely put on the right to data protection, with the hope that strengthening the protection offered by this right will address all the challenges to privacy. In several documents, the Article 29 Working Party (Article 29) has gone along those lines, for instance when it has advocated for the recourse to privacy by design.[22] In particular, Article 29 has put forth the need to enshrine in the revised data protection Directive the so-called principle of accountability, which would ensure a better application and implementation of the existing principles, by constraining data controllers to take appropriate and effective measures to implement data protection principles, and to demonstrate upon request that appropriate and effective measures have been taken.[23]

However critical and instrumental the accountability principle may be to an efficient implementation of data protection principles, this paper contends that as such it is not sufficient to effectively protect the privacy of citizens. An adequate protection must correctly articulate both the rights to data protection and to privacy, hence the need to return to privacy.

Once this premise is accepted, one still needs to determine how to best articulate the two rights.

In order to answer this question, the following lines are dedicated to a legal analysis of both the concepts of privacy and data protection from the point of view of the European legal order. They aim at better understanding the differences and interplays that exist between the legal notions of privacy and data protection.
Consequently, this paper will point at privacy and data protection as legal tools, produced, and constructed by European law.[24] Hence, our description of the *legal* construction of privacy and data protection will draw from an analysis of legal sources, and thus the pertinent case law, as it develops within the pertinent legislative framework (drawing inspiration from the interpretative and systematising work of legal scholars).[25] Constitutional theory will also be mobilised, as going back to the roots of the democratic constitutional State might provide further explanations on the different nature of the two rights.

The last section will outline the relevance of the distinction between privacy and data protection in the light of some contemporary challenges posed by ICTs.

---

[22] See, Article 29 Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN WP168, adopted on 01 December 2009.
[23] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, 00062/10/EN, WP 173, adopted on 13 July 2010. It is to be noted that though absent from Directive 95/46/EC, the principle of accountability is one of the eight core principles of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[24] The European framework, or European order refers to the EU legislation, and to some extent to the legal instruments that have been produced in the framework of the Council of Europe.
[25] The work of legal scholars will only be referred to if it helps in understanding the issues at hand.

2. Mapping the content of both rights

This section will outline the content of both the right to privacy and the right to data protection. After showing that the two rights can be differentiated from a formal viewpoint, it will engage in outlining their substance.

2.1 Privacy and data protection as two formally distinct rights

From a formal point of view, setting out the difference between privacy and data protection is a straightforward operation since the two notions are endorsed in two different fundamental (cf. fn 28) rights at the European level.

Privacy is enshrined in article 8.1 of the ECHR and article 7 of the EUCFR.[26] Both instruments protect everyone's "*right to respect for his private and family life, his home and his correspondence/*[communications in the case of the EUCFR]". This protection however, is not absolute according to the Convention. Article 8.2 lays down the conditions under which interferences with this right are allowed. Article 8.2 lays down three criteria of validity: the law must foresee the interference, it must be necessary in a democratic society (and proportionate), and it must pursue a legitimate aim.[27] Article 52.2 of the EUCFR provides for a similar limitation.[28]

Data Protection is enshrined in article 8 of the EUCFR, which states not only that "*Everyone has the right to the protection of personal data concerning him or her*", but also that "*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*." Finally, it also says that "*Compliance with these rules shall be subject to control by an independent authority.*"

In other words, the Charter distinguishes two rights of which the former concerns the *privacy of individuals* while the latter focuses on the *processing of personal data* and provides that such processing should be surrounded with (constitutional) safeguards. Hence, it appears quite clearly from the preceding paragraphs that privacy and data protection are indeed two distinct rights, at least formally.[29] But what about their

---

[26] EU Charter of Fundamental Rights, OJ, C 364/10, 18.12.2000; European Convention of Human Rights, www.echr.coe.int.

[27] Article 8.2 states 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*".

[28] Article 52.2 states that "*Rights recognised by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties.*"

[29] Some have even argued that they are two distinct fundamental rights. If the statute of privacy as a fundamental right is beyond controversy, that of data protection has been more discussed. However, it seems that the idea is gaining momentum since the consecration of the right to data protection in some national constitutions (Portugal, Spain) has been enhanced by its enshrinement at the European legal order level. See, Rodotà, S., "Data protection as a fundamental right", *in* Gutwirth, S., Poullet, Y., De Hert, P., de Terwagne, C., and Nouwt, S., (eds.), *Reinventing Data Protection?*, Dordrecht: Springer, 2009, pp. 77-82.

content, are they overlapping, or is there some space for differences?

2.2 A matter of substantial differences

Privacy. In order to understand the concrete meaning of the general (and abstract) right to privacy, one needs to look at how the European Court of Human Rights (ECtHR) has substantiated it through its case law.
Since Art. 7 EUCFR is a replica of Art. 8 ECHR, at European level the *content* of privacy for legal purposes can be securely derived from the pertinent case law of the European Court of Human Rights in Strasbourg (ECtHR). The court has guaranteed the protection of the four-folded right to privacy – private life, family life, home, and correspondence, enshrined in the ECHR, and very much inspired by the Universal Declaration of Human Rights,[30](which understands privacy as the protection of the sphere of people's intimacy, or the right for people to live free from arbitrary interferences in their "private sphere").[31]
In this respect, the Court has ruled that art. 8 ECHR can cover a wide range of issues such as integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data,[32] wiretapping, gender, health, identity (i.e., a right to have some control over biographical data such as one's name), protection against environmental nuisances and so on: the list is not exhaustive.[33] But the Court went further and also implied that privacy is a relational concept that reaches well beyond a mere right to intimacy, with the important consequence that art. 8 ECHR may also protect visible features and the public conduct of individuals (public privacy).[34] Progressively, the Strasbourg Court also acknowledged the right to make essential personal choices (such as name and sexual orientation) and eventually this has led the Court to state that individual self-determination or autonomy is an important principle underlying its interpretation of art. 8 ECHR.[35] Such an evolution has led the Court to ascertain that it is neither

[30] Article 12 of the Declaration states that: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation*".
[31] It has been argued that the wording of the Universal Declaration, and hence, that of the European Convention have been inspired by the seminal article of Warren and Brandeis on privacy as "the right to be let alone". This in turn, provides an historical understanding of how the case law of the European Court, and of its evolution. See, Sudre, F., "Rapport Introductif: La 'Construction' Par Le Juge Européen Du Droit Au Respect De La Vie Privée," *in* Sudre, F., (eds), *Le Droit Au Respect De La Vie Privée Au Sens De La Convention Européenne Des Droits De L'homme*, Brussels: Bruylant, Nemesis, 2005, pp. 1 and following.
[32] Cf. *infra*.
[33] And is not meant to be.
[34] E.g. *Rotaru vs Romania* of 4 May 2000, § 43; *P.G. & J.H. vs U.K.*, of 25 September 2001, § 57, *Peck vs U.K.,*of 28 January 2003, § 58.
[35] *Pretty vs U.K.,* of 29 April 2002, § 61, Judgment: "As the Court has had previous occasion to remark, the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (X. and Y. v. the Netherlands judgment of 26 March 1985, *Series A* no. 91, p. 11, § 22). It can sometimes embrace aspects of an individual's physical and social identity (Mikulic v. Croatia, no. 53176/99 [Sect. 1], judgment of 7 February 2002, § 53). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see e.g. the B. v. France judgment of 25 March 1992, *Series A* no. 232-C, § 63; the Burghartz v. Switzerland judgment of 22 February 1994, *Series A* no. 280-B, § 24; the Dudgeon v. the United Kingdom judgment of 22 October 1991, *Series A* no. 45, § 41, and the Laskey, Jaggard and Brown v. the United Kingdom judgment of 19 February 1997, Reports 1997-1, § 36). Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz v.

possible nor necessary to determine the content of privacy in an exhaustive way,[36] which is extremely consistent with the observation that the Court seems to favour a "liberty" rather than a "bundle of subjective rights" approach to privacy.[37][38]

Data Protection. Whereas the fundamental right to privacy is, as seen above, formulated in general terms, the more recent explicit recognition of the fundamental right to data protection in generic terms in the EUCFR has been preceded, since the late 1970s, by abundant international, European and national legislation (cf. *supra*, OECD guidelines and CoE Convention 108, but also many national statutes).

At European level the most important instrument is the Data Protection Directive, which is especially important because it introduced data protection principles within EU legislation and set the main benchmarks for the protection of personal data in following EU instruments. Furthermore, its transposition in national legal frameworks of Member States partially streamlined national legislation, and also provided the occasion to develop new, specific, legislations.[39]

As far as its scope is concerned, the Directive covers data protection within community law (the ex first pillar) and establishes the principles of protecting the individual's right to privacy while ensuring the free flow of personal data (art. 1.1 and 1.2). According to its article 2, however, it covers the processing of personal data understood as "any information relating to an identified or identifiable natural person ('data subject')".[40]

With respect to the core content of the right to data protection, Directive 95/46/EC provides principles regarding the processing of personal data, rights for data subjects,

---

Switzerland, Commission's report, op. cit., § 47; Friedl v. Austria, *Series A* no. 305-B, Commission's report, § 45). Though no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees. " See also Evans vs. United Kingdom, of 10 April 2007, § 71: "The Grand Chamber agrees (…) that "private life" is a broad term encompassing, *inter alia*, aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world (see *Pretty,* cited above, § 61)", we underline; Odièvre vs. France, of 13 February 2003, §29: "The Court reiterates in that connection that "Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. ... The preservation of mental stability is in that context an indispensable precondition to effective enjoyment of the right to respect for private life" (see *Bensaid v. the United Kingdom*, no. 44599/98, § 47, ECHR 2001-I)".

[36] *Niemietz vs. Germany* of 16 December 1992, § 29 and *Pretty vs. U.K.,* of 29 April 2002, Judgment: "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."

[37] Rigaux, F., (ed.), *La vie privée, une liberté parmis les autres?*, Larcier, Brussels, 1992; Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, 2002.

[38] Such an approach is equally consistent with Isaiah Berlin's work on positive and negative freedom, see, Sir Berlin, I., *Four essays on liberty*, Oxford: Oxford University Press, 1969.

[39] De Hert, P., and Bellanova, R., 2009, *op. cit.*, p. 7.

[40] Article 2(a) states that "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

and obligations for data controllers. In article 7, the Directive establishes a number of quintessential conditions for personal data to be processed legally, amongst which the "unambiguous consent of the data subject" and/or the fact that the processing serves "legitimate interests pursued by private interests". The Directive further enacts a number of principles such as the purpose specification principle (the processing and use of data for specified, explicit and legitimate purposes), the fairness principle (all processing must be fair and lawful to the data subject) or the data quality principle (all data must be adequate, relevant and not excessive in relation to the purpose for which they are processed). Regarding sensitive data as mentioned in art. 8, the regime is stricter and, in principle, prohibitive. Data subjects are endowed with a number of subjective rights (such as the right to receive some information whenever data is collected, to access the data, to have data corrected, and to object to certain types of processing), whilst some obligations are imposed upon data processors, who must guarantee the confidentiality of data against unauthorised access and, in some cases, must notify a specific independent supervisory body before carrying out certain types of data processing.

The right to data protection can thus be understood as a set of "Fair Information Practices"[41] which are complemented by other articles of the directive providing for an institutional framework designed to monitor the effective implementation of the directive and/or act as advisory bodies. In this respect, article 28 of the Directive foresees the setting-up of national data protection authorities (supervisory authorities or "DPAs"-data protection authorities). They are entrusted with several tasks such as keeping a processing register, offer advice, investigate issues, handle complaints, take certain decisions concerning particular processing operations, provide authorisations, issue binding regulation, or even take some cases before Courts. Article 29 of the directive creates the Article 29 Working Party, a sort of "derivative" institution that provides for coordination among independent data protection authorities and enhances their role at EU level (González-Fuster and Paepe, 2008, Poullet and Gutwirth, 2008). The Regulation 45/2001/EC is also relevant in this context, because it created the European Data Protection Supervisor, an autonomous EU institution with the powers of supervision, consultation and co-operation (art. 41).

As a conclusion, it transpires from the data protection regulation that its aim "*consists in providing various specific procedural safeguards to protect individuals' privacy and in promoting accountability by government and private record-holders*" (De Hert and Gutwirth, 2006). Data protection legislation does not aim at stopping or limiting data processing. On the contrary, its fundamental aim is to allow for the free flow of (personal) information, but being aware of the sensitive nature of such a process, it has deemed essential to put in place safeguards for the citizens' fundamental rights.

3. Interplays

[41] This expression is mainly used in US literature, see for example, Schwartz, P., M., and Treanor, W., M., "The New Privacy", *Michigan Law Review*, vol. 101, 2003, pp. 2163-2184. However, Bennett and Raab confirm us that it is not limited to US law, as they also frame EU data protection legislation in terms of Fair Information Practices, see, Bennett, Colin, J., Raab, Charles, D., *The Governance of Privacy – Policy Instruments in a global perspective*, Cambridge, London: The MIT Press, 2006, pp. 12-13.

It follows from the preceding paragraph that the legal rights to privacy and data protection differ not only from a formal view (the legislation distinguishes the two rights and enshrines them in different provisions and or instruments), but also from a substantial viewpoint. Indeed, whereas privacy protects a non-exhaustive list of prerogatives (ranging from the protection of the domicile to the right for a person to choose his/her sexual orientation), data protection regulates the processing of personal data, i.e. data relating to an individual, submitting it to obligations for data controllers and rights for data subjects.

However, the fact that privacy and data protection are two different rights doesn't mean they are impermeably separated. On the contrary, as evidenced by the case law of the ECtHR and of the European Court of Justice (ECJ), there are many interplays and overlaps. This section will outline these similarities and explain them by referring to the broader political framework in which they operate: the democratic constitutional State.

3.1 Overlaps

As a matter of fact, complaints concerning the processing of personal data have effectively been filed before the ECtHR. But since the European Convention of Human Rights contains no provision relating to data protection, the Court had to rule such cases within the framework of article 8 of the Convention (i.e. the right to privacy). It has therefore developed a set of criteria to determine whether a given processing of personal data can be encompassed within the right to privacy or not.

To that end the Court distinguishes between the processing of data that concern the private life and the processing of data that do not. It uses two criteria to make the distinction: the nature of the data processed and the extent of the processing. If the data are intrinsically linked to the private life of the individual, then the processing will fall under article 8 of the ECHR without. If the data are not "essentially private", the Court will look at the extent of the processing: does it systematically store the data? Does it store the data, though not systematically, but with a focus on the data subject? Could the data subject not reasonably expect the processing? In a number of cases, the Court has condoned data processing with regard to issues pertaining to the privacy of the data subject,[42] but not in all cases.[43] It can therefore be inferred from this case law that unlike data protection, which applies every time personal data are processed, the legal right to privacy stemming from article 8 of the ECHR does not. Consequently, this entails that not every processing of personal data necessarily affects privacy, although it is nonetheless covered by data protection legislation.

Where the Strasbourg Court has acknowledged that a data protection issue is also a privacy issue, it has granted some of the guarantees provided by data protection

[42] *Amann vs Switzerland* of 16 February 2000, § 65, *Rotaru vs Romania* of 4 May 2000, § 43; *P.G. & J.H. vs U.K.*, of 25 September 2001, § 57. See also De Hert, P., and S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing data protection?*, Springer, Dordrecht, 2009, pp. 3-44.

[43] De Hert, P., and Gutwirth, S., 2009, pp. 20-26.

legislations: it has acknowledged a right to access to personal files[44], accepted claims regarding the deletion of personal data contained in public dossiers[45] and the correction of "official sexual data" from transsexuals[46]; it has further insisted upon the necessity of having independent supervisory authorities in the context of the processing of personal data[47]; it endorsed the principle of purpose limitation when it ruled that personal data cannot be used beyond normally foreseeable use[48], and the principle that governmental authorities may only collect relevant data based on concrete suspicions[49]. Finally, the Court acknowledged the right to financial redress in the case of a breach of article 8 caused by the processing of personal data.[50] But even though the Court has consecrated some of the data protection principles (that mainly stem from Convention 108 and the Data Protection Directive) in its rulings, the case-by-case approach, could never have lead to a result similar to the systematic and general nature of data protection law.

The ECJ, on the other hand, is competent to make rulings concerning conflicts based upon the Data Protection Directive. Some of its cases have been permeated by a "privacy logic". It has stated that the processing of personal data can affect the right to privacy. Therefore, provisions of the Directive that might affect this right must be interpreted in the light of art. 8 ECHR,[51] and pass the threefold threshold test foreseen by the article,[52] although Member States enjoy a wide margin of appreciation.[53] In its first judgement, the Court went so far as to declare that an unlawful data processing is equal to a breach of privacy.[54] References to the threefold test of the ECHR were also made in other cases.[55] However, in more recent cases, the European Court of First Instance has reminded us that "the mere presence of the name of a person in a list of participants at a meeting does not compromise the protection of the privacy of the person",[56] thereby echoing the case-law of the ECtHR.

Finally, it is important to underline that, from a conceptual perspective, data

[44] ECtHR, *Gaskin v. the United Kingdom*, Application No. 10454/83, Judgment of 7 July 1989; ECtHR, *Antony and Margaret McMichael v. United Kingdom*, Application No. 16424/90, Judgment of 24 February 1995. ECtHR, *Guerra v Italy*, Judgment of 19 February 1998, *Reports*, 1998-I; ECtHR, *McGinley & Egan v. United Kingdom*, Applications nos. 21825/93 and 23414/94, Judgment of 28 January 2000.

[45] ECtHR, *Leander v. Sweden*, Application No. 9248/81, Judgment of 26 March 1987; ECtHR, *Segerstedt-Wiberg and others v. Sweden*, Application No. 62332/00, Judgment of 6 June 2006.

[46] ECtHR, *Rees v UK*, Judgment of 25 October 1986 *Series A*, No. 106; ECtHR, *Cossey v UK*, Judgment of 27 September 1990, *Series A*, No. 184; ECtHR, *B v France*, Judgment of 25 March 1992 *Series A*, No. 232-C; ECtHR, *Christine Goodwin v. the United Kingdom*, Application No. 28957/95, Judgment of 11 July 2002.

[47] ECtHR, *Klass v. Germany*, § 55; ECtHR, *Leander v. Sweden*, §§ 65–67; ECtHR, *Rotaru v. Romania*, §§ 59–60. See in detail: *Gaskin v. the United Kingdom*, Application No. 10454/83, Judgment of 7 July 1989; ECtHR, *Z. v Finland*, Application No. 22009/93, Judgment of 25 February 1997.

[48] ECtHR, *Peck v. the United Kingdom*, § 62; ECtHR, *Perry v. the United Kingdom*, § 40; ECtHR, *P.G. and J.H. v. the United Kingdom*, § 59.

[49] *Amann v. Switzerland*, § 61 and § 75 ff.; ECtHR, *Segerstedt-Wiberg v. Sweden*, § 79.

[50] *Rotaru v. Romania*, § 83.

[51] ECJ, Österreichischer Rundfunk, §. 68

[52] ECJ, Österreichischer Rundfunk, §. 83

[53] ECJ, Österreichischer Rundfunk, §. 83

[54] ECJ, Österreichischer Rundfunk, §. 91.

[55] See Opinion of the Advocate General Leger in Cases C-317/04 and C-318/04, §. 229.

[56] ECtFInstance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, §§. 114-115.

protection is both broader and narrower than privacy. It is narrower because it only deals with personal data, whereas the scope of privacy is wider. It is broader, however, because the processing of personal data can have consequences not only in terms of privacy, but also in terms of other constitutional rights. For example, data processing can impact upon people's freedom of expression, freedom of religion and conscience, voting rights, etc. Most importantly, the knowledge of individuals that can be inferred from their personal data may also bear risks in terms of discrimination.

3.2 A broader referential: the democratic constitutional State

In trying to make sense of such an ambiguous relation, we deem it useful to refer to the broader constitutional framework within which both rights operate: the democratic constitutional State. Indeed, contrary to previous political systems characterised by an authoritarian ruler, the very aim of democratic regimes is to guarantee personal freedom and self-determination while at the same time preserving order. It is thus in constant tension, since it has to preserve simultaneously two antagonistic values (individual liberty *versus* order).[57]

In order to reach this objective, democratic constitutional States have created a political structure wherein power is limited and non absolute, and which resorts to a double constitutional architecture. On the one hand, fundamental freedoms/human rights empower citizens with a set of individual rights that limit and counterbalance the power of the State. On the other hand, the power of the State is subject to constitutional rules holding the government to its own rules and to a system of mutual checks and balances (rule of law, transparency, accountability). Furthermore, governments will be legitimate if and only if they can be considered as an expression of the "will of the people" (i.e., representation through elections).[58]

Such architecture is thus not only based upon the assumption that citizens are "autochthonous" (they were already "there" before the state) and autonomous political actors, but it also constitutionally enforces it. By shielding individuals from abuses of power through human rights, and by controlling this power with checks and balances, and transparency and accountability, it has contributed to the constitutional creation of the political private sphere. This political space is antagonistic –though also articulated upon- the political public sphere, where government and State intervention are legitimate.[59]

As a matter of fact, it is interesting to notice that the legal right to privacy has been elaborated as an answer to the gaps and weaknesses detected in the protection of the political private sphere as it was ensured prior to the advent of this right by the other, more classical human rights (e.g., prohibition of torture, freedom from arbitrary arrest,

---

[57] De Hert, P., Gutwirth. S., "Regulating profiling in a democratic constitutional state", *in* M. Hildebrandt, M., and Gutwirth, S., (eds), *Profiling the European citizen. Cross disciplinary perspectives*. Dordrecht, Springer, 2008, p. 271-291.

[58] De Hert, P., Gutwirth. S., "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power", *in* Claes, E., Duff, A., and Gutwirth, S., (eds), *Privacy and the Criminal Law*, Antwerp/Oxford: Intersentia, 2006, pp. 61-104.

[59] Gutwirth, Serge, "De polyfonie van de democratische rechtsstaat", in Elchardus, M. (ed.), Wantrouwen en onbehagen, VUB Press, Brussels, 1998, pp. 137-193; De Hert, P., and Gutwirth, S., 2006, *op. cit*.

freedom of expression). In this sense, the right to privacy can be considered as a residual protection of the political private sphere against unlawful interferences, and hence, the ultimate defence line of liberty.[60]

Thus, both the fundamental rights to privacy and data protection protect the political private sphere, although in different ways.

Privacy can be conceptualised as an *opacity tool*, i.e., a – highly normatively embedded – constitutional tool that sets the limits that determine whether an interference with individual autonomy is acceptable or not. The regime they install is that of a **principled proscription**: interferences are forbidden except in peculiar situations and under stringent conditions whereby they are tolerated.[61] The right to privacy, which protects, *inter alia*, the inviolability of individuals' home, or their sexual preferences, operates within this constitutional setting.

Data protection on the contrary can be framed as a *transparency tool*, i.e., a constitutional that tends to guarantee the transparency and accountability of the power wielder. Indeed, whereas *opacity tools* embody normative choices about the limits of power, *transparency tools* come into play after these normative choices have been made, in order to channel the normatively accepted exercise of power through the use of safeguards and guarantees in terms of accountability and transparency. Data protection legislations do obey this transparency logic: by default they do not dispute the fact that personal data may be processed, but they create supervisory bodies and empower data subjects with subjective rights in order to make sure that data processors don't abuse their powers (which are bound by their obligations and the principles that govern the processing of such data).[62]

As a conclusion, privacy and data protection are both legal instruments designed to protect the political private sphere. However, they do so through different means (one by determining the legal dimension of the political private sphere, the other by protecting it), and consequently, their respective legal content differ as well.

4. Practical consequences of the distinction: threats in the ICTs framework

This final section will outline the relevance of the distinction that has been made between the two different legal constructions in the light of some of the challenges that ICTs pose. It will show that in the face of these challenges, a renewed appropriation of this distinction might produce better results than solutions strictly limited to the right of data protection (as is the case of the principle of accountability for instance).

The dangers stemming from ICTs are not new and well known. As a matter of fact, ICTs have led individuals to leave a huge number of traces that are detectable, (re)traceable and correlatable far beyond their control. Each time individuals use a network they leave digital traces. In other words, "today... an individual leaves a vast

[60] De Hert, P., and S. Gutwirth, 2008, *op. cit*.
[61] *Op. cit*.
[62] cf. *supra* 2.2.

amount of processable electronic traces in his wake".[63] They become the resources of a very extensive network of profiling devices that generates knowledge concerning and/or affecting the persons who leave these traces. Such practices of data mining and profiling entail several risks in terms of privacy, mainly a loss of individual autonomy.

Because of the massive capacities and capabilities of contemporary technologies, a huge amount of information concerning a single individual can be mined, and on the basis of this mining, predictions can be made about the future behaviour of this person. This becomes even more possible with the linkages of different databases and the convergence of technologies. The recourse to profiling is at work in almost all sectors of society. This is the metaphor of Franz Kafka's *The Trial*. In this epic novel, citizens are at the mercy of a bureaucratised world whose opaque functioning they fail to understand. Not knowing what is happening to them or why, they have no control over their own destinies. Decisions are based upon people's dossier and data and they have no chance to contest. They are helpless.[64] There lies the danger: normalisation and customisation of people's conduct (their conduct is being steered by others),[65] [66] a loss of control, and a sharpening of (informational) power inequalities (users don't know who processes their data and how their data is being used by others). A specific danger in that respect is the development of unsolicited communications and adjustments. Unsolicited communication refers to unsolicited commercial communication through automatic and intrusive means. A good example is spam. Unsolicited communications are not new[67] and are evolving into unsolicited adjustments. Such things already happen, as is the case with Amazon's book recommendation system, which collects information about customers' tastes in order to provide them guidance on which other items to buy. This might ultimately lead to "adaptative environment scenarios" where the loss of liberty and autonomy of the individual takes proportions that would have been unthinkable just a few years ago.[68]

In our view such threats unleash an important legal challenge as far as data protection legislation is concerned. We have seen that the scope of data protection concerns all, but only, personal data, understood as individuals' *biographical data*.[69] Nonetheless, just as the ICT world has its own architecture, it also has its own kind of data. Indeed, many of the data left by users on networks are not *biographical* in the legal sense. However, and although they do not identify users, these type of data enable a data processor to track the user and to identify him/her, since they reveal the type, duration

[63] De Hert, P., and S. Gutwirth, "Regulating profiling in a democratic constitutional state", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European citizen: Cross disciplinary perspectives*, Springer**,** Dordrecht, 2008, pp. 271-291.

[64] Solove, Daniel, "The Digital Person and the Future of Privacy", in Katherine J. Strandburg and Daniela Stan Raicu (eds.), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer, 2006, pp. 3-13; also *in* Pérez-Asinari, M.V., and P. Palazzi (ed.), "Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law", Bruylant**,** Brussels, 2008, pp. 355-365.

[65] De Hert and Gutwirth, 2008, op. cit.

[66] De Hert and Gutwirth, 2008, op. cit.; Poullet, Yves, "About the E-Privacy Directive: towards a third generation of data protection legislation?", in Serge Gutwirth, Yves Poullet and Paul de Hert (eds.), *Data Protection in a Profiled World*, Springer, Dordrecht, 2010, pp. 3-30.

[67] And are regulated through Directives 97/7/EC, 97/66/EC, 2000/31/EC, and 2002/58/EC.

[68] See, Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., Punie, Y., (eds), *Safeguards in a World of Ambien Intelligence*, Dordrecht: Springer, 2008.

[69] Poullet, 2010, op cit.

of communications, the frequency a user connects to a network, etc. This is the case for cookies, IP addresses or RFID tag numbers, which are associated with a site or an object to which a person connects. Are these personal data? And is personal data the adequate concept since profilers using this kind of data don't need to identify the user behind the traces that he/she has left behind (what is needed is the operations undertaken by the user, which this kind of data reveals, without need to identify the user)[70]. Is data protection able to cope with these changes?

The question might be asked as to whether the accountability principle represents a sustainable solution to these challenges. If it is not contested that the privacy of citizens will benefit from concrete and effective measures that will lead to a better implementation and respect of data protection legislation, this is, once again, not enough, as the very relevance of the personal data protection framework is jeopardized by ICT developments.

The European Union seemed to be aware of these issues when it introduced the (amended) E-Privacy Directive.[71] According to its art. 1.2, the Directive particularises and complements the Data Protection Directive in the electronic communications sector.[72] However, in doing so, the Directive goes beyond a mere implementation of the data protection principles, and seems to somewhat twist them. For instance, it introduces two kinds of data that are not personal: traffic data[73] and location data.[74] Equally, the Directive shifts from the regulation of the data controller to that of the providers of a publicly available electronic communication service, no matter whether the latter have been involved in operations of personal data processing.[75]

Both these solutions demonstrate –or so we contend, the impasse of a legal framework that puts the regulatory emphasis solely upon data protection legislation.
It is undisputed that the practices described above raise challenges for privacy understood as information control. However, these threats go well beyond mere issues of control over information as they threaten to shrink the autonomy and liberty of citizens. This conclusion should lead us to realise that data protection legislation, which has been somewhat understood as the legal translation of the "privacy as

[70] Poullet, Yves, "Pour une troisième generation de règlementation de protection des données Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law", *in* M.V. Pérez-Asinari and P. Palazzi (eds.), Brussels, Bruylant, 2008, pp. 25-70.

[71] Directive 2002/58/EC on privacy and electronic communications, OJ L 201/37, 31.07.2002, as amended by Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006; and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending, inter alia, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 337 8.12.2009.

[72] Directive 2002/58/EC, art. 1.2: "The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1".

[73] "Any data processed for the purpose of the conveyance of a communication on an electronic communication network, or for the billing thereof".

[74] "Any data processed in an electronic communications network, indicating the geographical position of the terminal equipment of a user of a publicly available electronic communication services".

[75] Rosier, K., "La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative à au traitement des données à caractère personnel: comment les (ré)concilier?", in *Défis du droit à la protection de la vie privée*, Cahiers du C.R.I.D. n°31, Bruxelles, Bruylant, 2008, pp. 328-352.

informational control" conceptualisation, might not be able to counter these threats alone. Therefore, if we are serious about achieving the goal of data protection legislation (i.e., protecting the political private sphere), there needs to be a renewed interest in the legal right to privacy. Indeed, most of the issues at hand concern threats to the autonomy of the individual that fall within the realm of the right to privacy, but outside the scope of the right to data protection. Consequently, focusing on transparency-based (i.e., data protection-based) solutions, no matter how well intentioned they are (e.g., better implementing the legal framework), will always fall short of efficiently protecting the privacy of citizens. Instead, it is crucial not to equate privacy and data protection (at least from a legal viewpoint), and not to assume that the protection of privacy can be ensured solely from a data protection viewpoint. This is all the more crucial since the two regimes are intrinsically different (cf. opacity *vs.* transparency), and it is essentially the opacity regime of privacy that can set thresholds regarding the principled acceptability or not of new ICT-linked practices. Consequently, a renewed interest in privacy beyond data protection is essential if we want to keep intact the political private sphere of liberty. The latter entails the return to the more normative privacy test, which will be instrumental in protecting the autonomy of citizens, *inter alia*, by determining which practices that impact upon this very autonomy are deemed to be acceptable in a democratic constitutional State.

However, that is not to say that the principle of accountability is irrelevant for the protection of privacy and that it should thus be discarded. It is important to recall that so far, all the references made to the principle of accountability concern the principle as it has been put forth by the Article 29 Working Party in its opinion 173, which solely envisages the right to data protection (i.e., the need for a controller to take appropriate and effective measures to implement data protection principles, and the need to demonstrate upon request that appropriate and effective measures have been taken). Whether accountability can also be useful in the realm of privacy, remains an issue to be inquired. Indeed, the main criticism of this article is not directed towards the principle of accountability as such, but towards the idea according to which the protection of individuals' privacy can be safeguarded solely through data protection, (and since accountability aims at better implementing data protection principles it would, *ipso facto*, better protect individuals' privacy) which is, as we hope to have shown, incorrect, since privacy and data protection do only partially overlap and are rooted in a different default principle (respectively "opacity" and "transparency").

Even if the default approach of privacy protection is prohibitive, such does not imply that transparency and, more specifically, accountability (which is a part of what we have called "transparency") do not have a role to play when the right to privacy is at stake. What this would mean as to the concrete substantiation of the principle yet remains to be inquired. In this respect, the case law of the ECtHR might offer some guidance: accountability can probably be construed as a condition for legitimate restrictions of the right to privacy such as foreseen by art. 8.2 ECHR. For instance, in the Klass and Kruslin cases, the Court spelled out some accountability related requirement that states should take in order to ensure the lawfulness of telephone tapping.[76]

As a conclusion, it can be said that the principle of accountability can indeed be

[76] ECtHR, *Klass v. Germany*, §§ 49-60; ECtHR, *Kruslin v. France*, §§ 30-36, in particular §30.

instrumental in providing a better protection of European citizens' privacy, provided it is part of a broader legal framework that makes a skilful articulation and use of both tools of opacity and transparency, namely, the legal rights to privacy and of data protection.

5. Bibliography

Agre, Ph., E., M., Rotenberg, *Technology and Privacy: The New Landscape*, Cambridge, MA: MIT Press, 1997.

Article 29 Working Party, Opinion 3/2010 on the principle of accountability, 00062/10/EN, WP 173, adopted on 13 July 2010.

Article 29 Working Party, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN WP168, adopted on 01 December 2009.

Bennett, C., J., Ch., D., Raab, *The Governance of Privacy – Policy Instruments in a global perspective*, Cambridge, London: The MIT Press, 2006.

Berlin, I., *Four essays on liberty*, Oxford: Oxford University Press, 1969.

De Hert, P., and S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in Gutwirth, S., Y., Poullet, P., De Hert, C., de Terwagne, and S., Nouwt, (eds.), *Reinventing data protection?*, Springer**,** Dordrecht, 2002, pp. 3-44.

De Hert, P., R., Bellanova, *Data Protection in the Area of Freedom, Security and Justice: A System Still to Be Fully Developed?*, Brussels: European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 2009.

De Hert, P., S., Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power", *in* Claes, E., A., Duff, and S., Gutwirth, (eds), *Privacy and the Criminal Law*, Antwerp/Oxford: Intersentia, 2006, pp. 61-104.

De Hert, P., S., Gutwirth. "Regulating profiling in a democratic constitutional state", *in* Hildebrandt, M., and S., Gutwirth, (eds), *Profiling the European citizen. Cross disciplinary perspectives*. Dordrecht, Springer, 2008, p. 271-291.

European Parliament and the Council, Directive 95/46/EC 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 L 281, 23.11.1995.

Guild, E., S., Carrera, "The European Union's Area of Freedom, Security and Justice Ten Years On", *in* Guild, E., S., Carrera, A., Eggenschwiler, (eds), *The European Union's Area of Freedom, Security and Justice Ten Years On - Successes and future challenges under the Stockholm Programme*, Brussels, European Union and Centre for European Policy Studies**,** 2010, pp. 1-12.

Gutwirth, S., *Privacy in the information age*, Lanham: Rowman & Littlefield, 2002.

Gutwirth, Serge, "De polyfonie van de democratische rechtsstaat", in Elchardus, M. (ed.), Wantrouwen en onbehagen, VUB Press, Brussels, 1998, pp. 137-193.

Nissenbaum, H., *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford: Stanford Law Books, 2010.

Poullet, Y., "About the E-Privacy Directive: towards a third generation of data protection legislation?", in Gutwirth, S., Y., Poullet and P. De Hert (eds.), *Data Protection in a Profiled World*, Springer, Dordrecht, 2010, pp. 3-30.

Poullet, Y., "Pour une troisième generation de règlementation de protection des données Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law", *in* Pérez-Asinari, M.,V., and P. Palazzi (eds.), Brussels,

Bruylant, 2008, pp. 25-70.
Rigaux, F., (ed.), *La vie privée, une liberté parmis les autres?*, Larcier, Brussels, 1992.
Rodotà, S., "Data protection as a fundamental right", *in* Gutwirth, S., Y., Poullet, P., De Hert, C., de Terwagne, and S., Nouwt, (eds.), *Reinventing Data Protection?*, Dordrecht: Springer, 2009, pp. 77-82.
Roosendaal, A., *We are all connected to Facebook… By Facebook!*, on file with the author, 2011.
Rosier, K., "La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative à au traitement des données à caractère personnel: comment les (ré)concilier?", in *Défis du droit à la protection de la vie privée*, Cahiers du C.R.I.D. n°31, Bruxelles, Bruylant, 2008, pp. 328-352.
Rouvroy, A., Y., Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", *in* Gutwirth, S., Y., Poullet, P., De Hert, C., de Terwagne, and S., Nouwt, (eds.), *Reinventing Data Protection?*, Dordrecht: Springer, 2009, pp. 45-76.
Schwartz, P., M., and W., M., Treanor, "The New Privacy", *Michigan Law Review*, vol. 101, 2003, pp. 2163-2184.
Solove, D., J., *Understanding Privacy*, London, Cambridge, MA: Harvard University Press, 2008.
Solove, Daniel, "The Digital Person and the Future of Privacy", in Strandburg, K., J., and D., S., Raicu (eds.), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer, 2006, pp. 3-13, also *in* Pérez-Asinari, M.V., and P. Palazzi, "Défis du droit à la protection de la vie privée - Challenges of Privacy and Data Protection Law", Bruylant**,** Brussels, 2008, pp. 355-365.
Sudre, F., "Rapport Introductif: La 'Construction' Par Le Juge Européen Du Droit Au Respect De La Vie Privée," *in* Sudre, F., (eds), *Le Droit Au Respect De La Vie Privée Au Sens De La Convention Européenne Des Droits De L'homme*, Brussels: Bruylant, Nemesis, 2005, pp. 1-15.
Warren, S., D., L.,D., Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. 4, n° 193, 1890, pp. 193-220.
Westin, A., *Privacy and Freedom*, New-York: Atheneum, 1967.
Wright D., P., De Hert, S., Gutwirth, "Are the OECD Guidelines at 30 showing their age?", *Communications of the ACM*, Vol. 54/2, February 2011, 119-127.
Wright, D., S., Gutwirth, M., Friedewald, E., Vildjiounaite, Y., Punie, (eds), *Safeguards in a World of Ambien Intelligence*, Dordrecht: Springer, 2008.