For academic use only
Please do always refer to the published version

GELLERT R. & S. GUTWIRTH, "The legal construction of privacy and data protection", *Computer Law & Security Review (CLSR)*, 2013, Vol. 29, 522-530 (ISSN 0267-3649)

The legal construction of privacy and data protection

Raphaël Gellert[1] & Serge Gutwirth[2]

Introduction: a legal construction?

In the EU-FP7 PRESCIENT project[3] we have devoted important efforts provide a multidisciplinary analysis of privacy and data protection (especially in D.1[4]). This approach is a consequence of our dismissal of the assumption that there is, eventually and behind all descriptions, such thing as an essence of privacy and data protection that each discipline tries to unveil as correctly as possible and that would provide the ultimate touchstone or benchmark to state if the descriptions proposed are right or wrong. Rather, we believe that privacy and data protection are *products* of distinct practices and 'regimes of enunciation', such as politics, law, ethics, economy, religion and so on, and that the challenge is not so much to find the foundational unity "behind" these, than it is to understand how, each being singular, they interact and articulate.[5] Consequently, we have analysed privacy and data protection from a legal, social, economical and ethical viewpoint and we have found that these perspectives each yield their own understanding of the notions, which also differ from one to another, may overlap at times, or not at all.

In the following paragraphs, we will however focus on the *legal* construction of privacy and data protection, which is characterised by the legal hermeneutics that

[1] Raphaël Gellert is Ph.D. candidate at the LSTS research group of the Vrije Universiteit Brussel, e-mail: raphael.gellert@vub.ac.be
[2] Serge Gutwirth is full professor at the Vrije Universiteit Brussel, and director of the LSTS research group, e-mail: serge.gutwirth@vub.ac.be
[3] Privacy and emergent sciences and technologies: http://www.prescient-project.eu/
[4] D.1 refers to PRESCIENT Deliverable 1, which can be accessed at the following address: http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf
[5] This stance is explained (see the references) in a.o. Gutwirth S., De Hert P. & De Sutter L., 'The trouble with technology regulation from a legal perspective. Why Lessig's 'optimal mix' will not work' in Brownsword R. & Yeung K., *Regulating Technologies*, Oxford, Hart Publishers, 2008, 193-218 ; Gutwirth S., "Composer avec du droit, des sciences et le mode technique: une exploration" in D. Le Métayer (éd.) *Les technologies de l'information au service des droits : opportunités, défis, limites*, Bruxelles, Bruylant, 2010, 24-42 and Gutwirth S, "Le contexte du droit ce sont ses sources formelles et les faits et moyens qui exigent son intervention", *Revue Interdisciplinaire d'Etudes Juridiques. Droit en contexte*, 2013 (currently in production).

"catch" cases, as it is practised by judges, referring to what continental lawyers call the formal sources of the law (legislation, case-law, legal doctrine, custom, general principles of law and equity). Given the European context of the project, we have focused upon the European legal order, stemming from the EU and, to a lesser extent, from the Council of Europe.

In this paper we will undertake to differentiate the two rights first from a formal, and second from a substantial perspective. Third, we will analyse what these differences mean in practice, through three case studies (which we will borrow from Prescient's D.2).[6] In the light of the differences between the rights, the last and fourth part will put forward some ideas as how to best articulate them. We will seek ways of articulation mainly based upon the two rights' scope, and qualitative and quantitative thresholds.[7] These articulations will lead to final reflections on the relationship between privacy and data protection and, more fundamentally, to the meaning of data protection as a fundamental right.

1. Privacy and data protection: two formally distinct rights

1.1. Privacy

Privacy is enshrined in article 8.1 of the Council of Europe's (CoE) European Convention for Human Rights (ECHR) and article 7 of the EU Charter for Fundamental Rights (EUCFR), which is binding since its entry into force of the Lisbon Treaty.[8] 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.[9] Article 52.1 of the EUCFR provides for a similar limitation.[10]

1.2. Data Protection

[6] D.2 refers to PRESCIENT Deliverable 2, which can be accessed at the following address: http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf

[7] In their contribution to this issue of *CLSR* Gonzalez Fuster and Gutwirth do complementarily analyse the different understandings of data protection, oscillating between a prohibitive understanding which principally aims at withholding personal data and prohibiting their processing on the one hand, and a permissive understanding which assumes that personal data in principle may and will be processed, but subject to the guarantees provided by law. Differently, our contribution focuses upon the differences between privacy and data protection, which we – that is our position – comprehend under its permissive assumption.

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

[9] 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*".

[10] Article 52.1 states that "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*"

A broad range of instruments consecrates the right to data protection. At EU (quasi) constitutional level, it is enshrined in Art. 16 TFEU.[11] Art. 8 EUCFR also provides for such a right.[12] At a broader (quasi) constitutional European level, data protection had already been hallowed by CoE's Convention 108 from 1981,[13] and by the OECD "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" from 1980 (though they are not binding).[14]

However, data protection is also enshrined in a series of (quasi-)legislative EU instruments, the most important of which is the Directive 95/46/EC known as the Data Protection Directive[15] that introduced data protection principles within EU law and set the main benchmarks for the protection of personal data in the EU.[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 the 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]

Finally, on 25 January 2012, the European Commission released two proposals: one for a general data protection that would replace the data protection directive (General

[11] Art. 16 TFEU states that: "Everyone has the right to the protection of their personal data" .
[12] Art. 8 EUCFR not only provides 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."
[13] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS no. 108, Strasbourg, 18 January 1981.
[14] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[15] 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* 281, 23.11.1995.
[16] 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.
[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. It is to be noted that in the so-called EU third pillar, a number of data processing systems are in place and regulated by specific agreements, e.g., VIS, SIS I and II, Prüm, CIS, etc…
[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37, 31.07.2002, as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006, p. 54, and by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337 8.12.2009, p.11.
[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.

Data Protection Regulation - GDPR),[20] another for a police and criminal justice data protection directive that would replace the Council framework decisions.[21]

In sum, EU-law formally distinguishes two different fundamental rights[22]: the right to *privacy of individuals* and *the right to data protection*. Hence, it clearly appears that those fundamental rights must at least be formally distinguished from each other. But what about their content: are they completely different or do they partly overlap?

2. Privacy and data protection: two substantially distinct rights

2.1. Privacy

In order to understand the concrete meaning of the right to privacy, one needs to look at how the European Court of Human Rights (ECtHR) has substantiated it through its case law. Moreover, 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).[23] This court has indeed a long track record in guaranteeing the protection of the four-folded right to privacy – private life, family life, home, and correspondence - as enshrined in the ECHR.

In this respect, the Court has ruled that art. 8 ECHR can cover a wide range of issues such as bodily integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data,[24] 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.[25] But the Court went further and approached privacy as 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").[26] Progressively, the Strasbourg Court also acknowledged the right to make essential personal choices (such as name and sexual orientation) and eventually this has led to the understanding that individual self-determination (or autonomy) is an important principle underlying its interpretation of art. 8 ECHR.[27] Consequently the Court ascertained that it is

[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 final.

[21] European Commission, A proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 January 2012, COM(2012) 10 final.

[22] 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.

[23] Not least because The EU Court of Justice's case law on fundamental rights has also been traditionally marked by its habit of refer for guidance and inspiration to the ECHR, and to ECtHR's case-law, and because Art. 52.3 of the EUCFR stipulates that, insofar as it contains rights corresponding to rights guaranteed by the ECHR, their meaning and scope shall be the same.

[24] Cf. *infra*.

[25] And is not meant to be.

[26] 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.

[27] *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

neither possible nor necessary to determine the content of privacy in an exhaustive way,[28] which is extremely consistent with the observation that the Strasbourg Court seems to favour a "liberty" rather than a "bundle of subjective rights" approach to privacy.[29]

2.2. Data Protection

The Data Protection Directive applies to the processing of personal data, the latter being understood broadly as "any information relating to an identified or identifiable natural person ('data subject')".[30] The Directive enacts the principles for the legitimate processing of personal data, it provides rights for data subjects and imposes obligations upon data controllers. In article 7 it lists a number grounds that legitimize a processing of personal data, such as the fact that the processing is necessary "for the performance of a task carried out in the public interest" or "for the purposes of the legitimate interests pursued by the controller".[31] The Directive further enshrines the main principles of data protection which are the purpose specification principle (the processing and use of data must happen 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 aimed at by art. 8, the regime is stricter and, in principle, prohibitive. Next to this, data subjects are endowed with a number of subjective rights (such as the right to

---

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. 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)".

[28] *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."

[29] 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.

[30] 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".

[31] The "unambiguous consent of the data subject" is also one of such grounds, but the real role of consent as a legitimating ground is not clear : see e.g. Gutwirth, S., "Short statement about the role of consent in the European data protection directive", 2012 available at: http://works.bepress.com/serge_gutwirth/80

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"[32] or as the regulation and organisation of the conditions under which personal data can be lawfully processed. These fair practices are further 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), which 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 (Art. 29 WP), a sort of "derivative" institution that provides for coordination among independent data protection authorities and enhances their role at EU level.[33] 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). It is clear that the DPA's were installed to counterweigh the general power imbalance between the data controllers and the data subjects, and that their role is to supplement and give more force to the early stage control by the "consumers/data subjects" and the ex-post factum control by the courts.

As it follows from Art. 1.1 Data Protection Directive, the aim of data protection is to regulate a specific practice, namely the processing of personal data.[34] Therefore, it can be argued that data protection *by default* accepts the processing of personal data; otherwise its aim would be void (how can one regulate a practice if it is not for granted that it takes place?). Yet, aware of the sensitive and potentially threatening nature of such a process, it has put in place a number of qualitative thresholds (namely the purpose specification principle, the data quality principle, and the need for a legitimate basis for a treatment), and procedural safeguards (i.e., quantitative thresholds), which are deemed sufficient to protect the individuals' liberty when data about him/her are processed.

2.3 Overlaps

[32] 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.

[33] Poullet, Y., Gutwirth, S., "The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration Of "Reflexive Governance"?", *in Défis Du Droit À La Protection De La Vie Privée-Challenges of Privacy and Data Protection Law*, Maria V. Pérez-Asinari and Pablo Palazzi, (eds.), Brussels: Bruylant, 2008, pp. 569-607.

[34] Art. 1.1 provides that the object of data protection is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

Even if European law clearly distinguishes between privacy and data protection, both in terms of form and content, they intersect. Whereas data protection applies "automatically" each time personal data are processed,[35] privacy will only encompass such a processing if the European Court of Human Rights (ECtHR) decides that the processing at stake represents an interference with one's right to privacy under art. 8 ECHR. As a matter of fact, complaints concerning the processing of personal data have been filed before the ECtHR. But since the ECHR 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 subsumed or not within the right to privacy.

To that end the Court distinguishes between the processing of data that concern the private life of individuals and those that do not, using two criteria: the nature of the data processed and the extent of the processing. If the data are intrinsically linked to the privacy of a person, then the processing will fall under article 8 of the ECHR without further ado. But 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 to the privacy of the data subjects because the extent of the processing was such that it interfered with their privacy,[36] but not in all cases.[37] This entails that not every processing of personal data necessarily affects privacy, even if 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 legislations: it has so recognized a right to access to personal files[38], accepted claims regarding the deletion of personal data contained in public dossiers[39] and the correction of "official sexual data" from transsexuals[40]; it has further insisted upon the necessity of having independent supervisory authorities in the context of the processing of personal data[41]; it endorsed the principle of purpose limitation when it ruled that personal data cannot be used beyond normally foreseeable use[42], and the

[35] Art. 3.1 of Directive 95/46/EC clearly states that: "This Directive shall apply to the processing of personal data (…)".
[36] *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.
[37] De Hert, P., and Gutwirth, S., 2009, pp. 20-26.
[38] 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.
[39] 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.
[40] 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.
[41] 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.
[42] 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.

principle that governmental authorities may only collect relevant data based on concrete suspicions[43]. Finally, the Court acknowledged the right to financial redress in the case of a breach of article 8 ECHR caused by the processing of personal data.[44]

All in all, data protection and privacy overlap on a mode whereby data protection is both broader and narrower than privacy. It is narrower because it only deals with the processing personal data, whereas the scope of privacy is wider. It is broader, however, because it applies to the processing of personal data, even if the latter does not infringe upon privacy. Privacy also is broader and narrower: it might apply to a processing of data which are not personal but nevertheless affects one's privacy, while it will not apply upon a processing of personal data which is not considered to infringe upon one's privacy. It can be said as well that a processing of personal data can have consequences not only in terms of privacy, but also in terms of other constitutional rights, and most obviously, when the processing of data relating to individuals bears risks in terms of discrimination.

3. Privacy and data protection interplays in three case-studies

So far we have seen that although different, privacy and data protection may overlap and apply to the same data processing situation. In the following lines, inspired by Prescient's second deliverable (D.2) we will analyse three cases so as to analyse whether the two rights apply, and in case they do, whether the protection afforded is the same.

3.1. Body scanners: non personal data

In the course of the debates about the privacy and data protection implications stemming from the use of body scanners, a contentious issue has been that of the applicability of data protection legislation. For instance, the European Commission has advocated the use of Privacy Enhancing Technologies with respect to body scanners, which would ensure that, "images analysed by a human reviewer are not linked to the identity of the screened person and are kept 100% anonymous".[45] This statement –as laudable as it is- indeed might jeopardize the applicability of the data protection legislative framework since the latter only applies to personal data[46] and using anonymous data might render them non-personal.

The fact that the images produced by the body scanners are anonymous does however not *ipso facto* entail that such data no longer qualify as personal anymore and thus would escape out of the reach of Data Protection Directive. The aim of using anonymous data is to render the individual to whom they relate unidentifiable. As the Art. 29 WP explains in its Opinion 4/2007 on the concept of personal data,[47]

[43] *Amann v. Switzerland*, § 61 and § 75 ff.; ECtHR, *Segerstedt-Wiberg v. Sweden*, § 79.
[44] *Rotaru v. Romania*, § 83.
[45] European Commission, Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM (2010) 311 final, Brussels 15 June 2010, p. 13.
[46] 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".
[47] Article 29 Working Party, Opinion 4/2007 on the concept of personal
data 4/2007, WP 13 adopted on20 June 2007.

anonymous data can be personal data if they can be related to an individual that can only be indirectly identified. The Working Party adds that, in conformity with Recital 26 of Directive 95/46/EC, in order to determine whether an individual is identifiable in an indirect manner "*account should be taken of all the means likely reasonable to be used* (…)".[48] This criterion should take into account all the factors at stake (e.g., cost of identification, purpose of processing, organisation of the processing, etc.). It is also a dynamic criterion (consider the state-of-the-art of the technology at the time of the processing). Hence, the At. 29 WP concludes that the assessment whether a set of data can be considered personal or not depends on the circumstances, entailing that a case-by-case analysis is required.[49]

In other words, anonymised images in body scanner must not necessarily be considered as non personal data, and if this were the case, then the goal of protecting individuals through the use of anonymous data, might actually result into the (unintended) consequence of depriving them from the protection of the whole data protection framework, which as such is paradoxical.

But then again, the latter is not to say that there will be no protection of the individuals through the fundamental right to privacy. Which in our opinion effectively will be the case because on the one hand the collection of bodily information through scanners touches upon the intimacy of the person and represents a strong interference with his/her autonomy, and on the other the data collected by body scanners – images naked bodies stripped from their clothes – are certainly privacy-sensitive and intimate. In other words, given the current state of legislation, body scans provide for a situation wherein the processing of intrinsically privacy-sensitive data might, if anonymized, escape to the reach of data protection, however, undiminished the protection under the fundamental right to privacy.

3.2 Human enhancement technologies: consent

Human enhancement technologies such as brain computer interface (BCI) and neuro-enhancement will enable us to concentrate upon the role of consent and the different legal meanings it can acquire depending on the applicable legislation. One of the main goals of BCI is to enable partially or fully paralyzed people to communicate and regain (some) control over their lives. In other words, BCI can be seen as a way to empower people.

As we have already showed, the ECtHR case law has gone on to conceptualise privacy as a relational concept well beyond its definition as a mere right to intimacy, ultimately leading to the important consequence 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".[50]Amongst others, this right to self-determination includes the right to gender identification, or the right to sexual orientation.[51] In this respect, it is interesting to observe that the

[48] Underlined by the Art. 29 WP.
[49] Opinion, 4/2007, pp. 12-16.
[50] Evans vs United Kingdom, 10 April 2007, § 71.
[51] See e.g. the B. v. France, 25 March 1992, Series A no. 232-C, § 63; Burghartz v. Switzerland, 22 February 1994, Series A no. 280-B, § 24; Dudgeon v. the United Kingdom, 22 October 1991, Series A no. 45, § 41; Laskey, Jaggard and Brown v. the United Kingdom, 19 February 1997, Reports 1997-1, § 36.

ECtHR has also declared that participating to S&M practices as a "victim" is in principle protected by article 8 ECHR, provided that the consent and the will of the "victim" are respected, in conformity with the habits, customs and rules of such practices.[52] Therefore, the choice of patients to willingly resort to BCI interfaces seems compatible with their right to privacy, even though it might result into the discovery and the disclosure of some of their most intimate information to others and, also, to themselves. As a matter of fact, these developments are equally pertinent for issues in neuro-enhancement.

As far as data protection is concerned, it can be argued that consent alone is not necessarily a sufficient basis to declare a data processing legitimate. Indeed, Art. 7(e) and (f) of Directive 95/46/EC justify the processing of personal data tending to the realisation of a legitimate aim of the processor. Consent (consecrated as a basis legitimizing a process by Art. 7(a)) can therefore only be conceived as an additional ground for processing, since the opposite would entail that it could legitimize processing that are illegitimate from the point of view of Art. 7(e) and (f).[53] For instance, it might be argued that the use of such data for commercial purposes is illegitimate. Such a reading of consent is consistent with the conceptualization of data protection as fostering the transparency and accountability of the data controller.

3.3. Whole genome sequencing: proportionality

The third case-study concerned the use of full genome data and their further storage into databases. In this case, the proportionality of such measure has to be assessed both according to the right to privacy and the right to the protection of personal data, and it might well be the case that the outcome of these two proportionality tests diverge. The proportionality test embedded within Art. 8.2 ECHR, and used to determine whether an interference with privacy is legitimate weighed to the aim that is pursued, is (or at least should be) a strong, normative, test; whereas the nature, content, and meaning of the proportionality test embedded in Art. 6.1(a) and 6.1(c) is still very much disputed.

Under Art. 8.2 ECHR a proportionality test can be performed in different fashions. A lenient proportionality test –embedded in the metaphor of the balance- suggests that proportionality is a zero-sum game, which suggests that upholding one right *per se* weakens the other. Such a proportionality test is doomed to weigh one interest *against* the other, and makes impossible the search of a *composition* or *reconciliation* whereby the different interests at stake are all preserved in an optimal way (which is respectful of the foundational principles of the democratic constitutional state). However, a strong proportionality test does effectively encompass such composition or reconciliation, since it includes the possibility of deciding that the restrictive measures at stake are unacceptable because they harm the essence of a fundamental right or of the constitutional order, even if it can be shown that the measures at stake can indeed effectively uphold another legitimate interest. In the work of the European Court of Human Rights, this exercise is known as the "necessary in a democratic

[52] *K.A. and A.D. v. Belgium*, 17 February 2005, § 85. On this case, see also, Gutwirth, S., De Hert, P., De seks is hard maar seks (dura sex sed sex). Het arrest K.A. en A.D. tegen België, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, from Panopticon, vol.26, n. 3, 2005, pp. 1-14.
[53] Cf. Gutwirth, S., "Short statement about the role of consent in the European data protection directive", 2012 available at: http://works.bepress.com/serge_gutwirth/80

state", which is a component of the broader proportionality test. The issue at stake, then, is not a "balancing" between two values, but an answer to the questions "How much erosion of a fundamental right is compatible with the democratic constitutional state in which fundamental rights are a constitutive element?", or, "In which society do we want to live?". This entails that another aspect of a stronger proportionality test consists in the obligation to explore if there are alternative measures that allow for the realisation of the legitimate interest in a way that does not affect the fundamental rights in the same way as the proposed measure. In other words, one must try to find a way to protect and enforce both values without loss of the fundamental rights.

Such a strong proportionality test imposes itself if the storage of full genetic data into a database is at stake. As a matter of fact, in its Marper case the Strasbourg court upheld that such storage by the British police was unlawful, not in the least because of the indeterminate storage period of the data.[54]

As far as the proportionality test included in data protection is concerned, the situation is unclear. The proportionality test provided by data protection can be described as follows. It includes both the question of (strict) proportionality, and the question of necessity.

The condition of necessity is embodied in the *purpose specification principle*, which requires that data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes" (art. 6(b)*DP*). The condition of proportionality *stricto sensu* is embodied in the *data quality principle*, which requires, *inter alia*, that the data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"(art. 6(c)*DP*). Furthermore, it is useful to remember that in addition to being proportional, a processing must also be legitimate according to Art. 7.[55]

Yet, it remains to be seen what this proportionality test mean in practice. In their contribution to the present issue González Fuster & Gutwirth depict the problematic use of the proportionality test by the ECJ in data protection cases. Without restating their discussion, it suffices to say that they point at one case where the Court undertook a particularly shallow test.[56] In this article however we would like to frame the discussion on the nature of the proportionality test by focussing upon the object of data protection. Without engaging into a discussion on the rather elusive meaning of "personal data protection",[57] it is enough for us now to state that the relation between data protection and other fundamental rights (and in particular the right to privacy) is far from crystal clear, as evidenced by Art. 1.1 of the directive.

This problematic relation between data protection and other fundamental rights is epitomised in the ECJ case law. In some cases, the Court seems to grant an ancillary

---

[54] *S. and Marper v. The U.K.*, 4 December 2008, § 72. See also : DE BEER D., DE HERT P., GONZALEZ FUSTER G. & GUTWIRTH S., 'Nouveaux éclairages de la notion de la notion de « donnée personnelle » et application audacieuse du critère de proportionnalité. Cour européenne des droits de l'homme Grande Chambre *S et Marper c. Royaume Uni*, 4 décembre 2008, *Revue Trimestrielle des Droits de l'Homme*, 81/2010, 141-161

[55] The two conditions are cumulative and not alternative, see, Gutwirth, 2002.

[56] Case 70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (24 November 2011), §53. Yet, they also point out the fact that the severity of the test might depend upon the issue at stake.

[57] For mor details, see the contribution of González Fuster & Gutwirth in this issue, as well as, González Fuster & Gellert, *op. cit*.

status to data protection: the aim of the right to data protection (referred to either in the Directive, either to in the Charter) is to ensure the protection of the citizens' right to privacy.[58] In the same vein, in the *Schecke* case, the Court asserted the existence of a what could be coined as a *sui generis* right, since it consecrated the right "to respect for private life with regard to the processing of personal data."[59] However, in other cases, the Court has been more inclined to underline the independence of the right to personal data protection. That was the case for instance in the *Bavarian Lager* case, where the Court of First Instance stated 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".[60] Similarly, in the *Deutsche Telecom* case, the Court unambiguously declared that the data protection directive was "designed to ensure, in the Member States, observance of the right to the protection of personal data"; thus without reference to the right to privacy.[61]

In other words, the Court hesitates between an ancillary –or instrumental- conception of data protection, and between an autonomous conception. Such differences might not be without consequences for the proportionality test to be undertaken in data protection issues.

Under an ancillary acceptation, it could be argued that the data protection proportionality test would be stronger since, data protection is instrumental to protecting privacy with respect to the processing of personal data. In other words, the (possible) violation of the right to privacy would be internalized within the data protection proportionality test (one could argue that there would be a proportionality test within a proportionality test, since a proportionality test is necessary to determine whether the right to privacy has been violated or not). In the *Rijkeboer* case, the ECJ mentioned the internal balancing at work in data protection (though it referred to it as privacy), since there is a balancing operation taking place, but the balancing does not concern two opposed fundamental freedoms, but rather a freedom (data protection) and a practice (the processing of personal data and the obligations associated to it).[62] In such a situation, privacy considerations would be internal to this already internal balance. Furthermore, the question can be asked as to whether such reasoning is valid for other fundamental freedoms. In the *Lindqvist* case, the ECJ emphasized indeed that data protection's purpose is to establish a fair balance between *any* right affected and the free flow of information.[63] In other words, respecting data protection would entail respecting *all* the fundamental rights at stake (which would be internalized within the data protection proportionality test).

Under an autonomous acceptation, that is, if data protection is not instrumental to other human rights, one could argue that the proportionality test would be more

[58] C-275/06, Promusicae v. Telefonica de Espana, § 63; C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy, Satamedia Oy, § 52; Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof v Österreichischer Rundfunk et al and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, especially §91. In the *Rundfunk*, the Court applied a proportionality test based upon that foreseen by Art. 8.2 of the EUCFR, whereas in other cases it applied the test described by González Fuster & Gutwirth in their contribution to the present volume. As a matter of fact, this issue is beyond our point.
[59] Supposedly enshrined in Art. 7 and 8 of the EUCFR. Joined Cases C-92/09 and C-93/09, Volker and Markus Schecke GBR and Hartmut Eifert v. Land Hessen, 9 November 2010, § 52.
[60] ECtFInstance, The Bavarian Lager Co. Ltd v Commission of the European Communities, §§. 114-115.
[61] C-543/09, Deutsche Telekom AG v Bundesrepublik Deutschland, §50.
[62] Rijkeboer, §64.
[63] C-101/01, (6 November 2003), *Lindqvist*, § 97.

lenient. In such a situation, a processing of data is not framed as an interference with a right (as is the case with privacy, hence the applicability of Art. 8.2 ECHR), since data protection, by default authorises the processing of data. Therefore, the balancing operation still concerns the conditions of legality of a processing, except that this processing is not seen anymore as an interference with the right. The balancing thus takes place *within* data protection and simply requires that the data processed are "adequate, relevant and not excessive in relation to the purposes for which they are collected", and are not collected for other purposes than the ones foreseen (weak, or lenient proportionality test).[64] As a matter of fact, the European Commission's proposal for a general data protection regulation (GDPR) seems favor a more autonomous version of the right to personal data protection, though it refers to a wording that is ambiguous.[65]

Such theoretical developments have been (at least implicitly) echoed in the discussion concerning data protection impact assessments and data protection by design (provided by Art. 33 and Art. 28 of the GDPR). Whereas in other legal cultures these tools are coined as "privacy impact assessments" and "privacy by design", the proposed regulation uses the data protection vocabulary. Discussions have thus gone on to question whether a DPIA will mean assessing the compatibility of a proposed data processing operation not only with the provisions of the directive, or if it also entails to assess compatibility with the right to privacy (and eventually the whole spectrum of human rights)?[66]

4. Conclusion: articulating the two rights

In this article we have argued that the rights to privacy and data protection are two distinct rights, both formally and substantially. Yet, there exist situations of overlap whereby they apply to a same situation. We have therefore tried to see if, when applied to a same situation, they produce the same legal outcome (in terms of legality of the situation). The results were not always the same, though some uncertainties remained as to the manner in which the rights should be applied.

Given these possible overlaps, the question arises as to the articulation of the two rights. Earlier on, we described the two rights as being respectively both broader and narrower. We believe such relation can serve as a matrix for articulation.

The most obvious venue for articulation is the scope *ratione materiae*. Case study 1 (on the use of anonymous images in body scanners) contrasts the diverging scopes (and also shows the limits) of a right that regulates a specific and determinate practice (i.e., the processing of personal data) *versus* a right wherein a fundamental freedom is enshrined. Another possibility is to (briefly) explore two additional venues, namely data protection lawss qualitative (case study 3) and quantitative (case study 2) thresholds for a lawful processing of personal data.

---

[64] Art. 6.1(c).

[65] Art. 1.2 states that: "This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data." Under this drafting, the two parts are not antithetical, and it looks as though the proposal has featured the two possibilities without daring to choose one.

[66] See, De Hert, 2012; Prescient, D.4. In the same vein, the EU Fundamental Rights Agency has underaken in 2010 a full human rights impact assessment on body scanners, available at the following address: http://fra.europa.eu/sites/default/files/fra_uploads/959-FRA_Opinions_Bodyscanners.pdf

As far as the qualitative conditions are concerned, it is not contested that the right to personal data protection accepts *by default* the processing of personal data.[67] Yet, the extent of these conditions is not clear. We have seen in the last case-study that this issue was closely determined by the relation between data protection and privacy (ancillary or autonomous), which is, one might argue, coextensive to the core content and object of the right.

Under an instrumental conception, it can be argued that the right to data protection could serve as a safeguard not only for privacy but also for all fundamental rights. Such an observation is consistent with the scope of data protection being both broader and narrower than that of privacy and rightly applying to processing of personal data that might not affect privacy but other rights instead. In its *Huber* case, the ECJ tackled the issue of a discriminatory inclusion in a database through the lens of data protection. In its reasoning, the Court linked the prohibition of discrimination to the proportionality test of directive 95/46/EC.[68] Such a case tends to confirm the instrumental nature of data protection, which would safeguard the different rights at stake by internalising them within its internal balancing/proportionality exercise. Could data protection be framed as the vehicle to safeguard fundamental freedoms with respect to innovations that apprehend humans through a digital form? And in any event, what role is then left for the other fundamental freedoms? Would it make any sense to perform an additional (not internalised) proportionality test?

Under an autonomous conception, on the contrary, data protection would not internalise fundamental rights issues within its internal balancing/proportionality test, entailing that its qualitative conditions would focus on the processing operation *stricto sensu*, and would therefore be quite lenient (which is logical and not necessarily a bad thing since, in this hypothesis, the proportionality test of the fundamental right at stake must simultaneously be undertaken).

As far as the quantitative/procedural conditions are concerned, precisely because it *by default* accepts the processing of personal data, the right to personal data protection features a highly developed set of procedures that ensure the transparency and accountability of the data controller. Furthermore, the right also applies horizontally (and not only towards the state).[69] On the other hand, and even though the ECtHR has consecrated some of the data protection guarantees in its rulings, this case-by-case approach has so far not been able to match the consistent, comprehensive, and legally enshrined set of safeguards featured by data protection law (this all the more true in view of the proposed regulation that puts great emphasis on the principle of accountability).

To conclude, in our opinion, the fundamental right to personal data protection is bound to overlap with other rights because instead of granting a "substantial" freedom (such as the secrecy of correspondence, freedom of speech, freedom of religion, etc.) it is limited to determine the extent to which an infringement on our (undetermined) liberty can go (in this case, the practice consisting in processing personal data). This contrasts starkly with other rights that both grant a "substantial" freedom and provide for the means to determine the limits of such freedom.

---

[67] Cf. Art. 1.1 of Directive 95/46/EC. See also, Gutwirth, 2002, chapter 5; see also, *supra*, section 2.2.
[68] *Huber v. Germany*, C-524/06, Judgment of 16 December 2008, §§ 65-68.
[69] According to Art. 2(d) of directive 95/46/EC, " 'controller' shall mean the natural or legal person, public authority, agency or any other body (…)".

This conceptual lens casts a new light on the observation we made beforehand according to which data protection and privacy are both broader and narrower than each other. Therefore, under a situation bound to feature overlaps, it remains crucial to articulate the rights by skilfully determining on a case-by-case basis which one offers the best protection.