

Published chapter
This version is for academic use only
Always refer to the published version

DE HERT P. & GUTWIRTH S., 'European Data Protection's constitutional project. Its problematic recognition in Strasbourg and Luxembourg' in GUTWIRTH S., Y. POULLET, P. DE HERT, J. NOUWT & C. DE TERWANGNE (Eds), *Reinventing data protection ?*, Springer Science, Dordrecht, 2009, 3-44

'Although the 'formal' protection of the right to respect for private life, at least in areas covered by the first pillar, is in essence relatively satisfactory, there are concerns surrounding the weakening of the 'substantial' protection of that right'.¹

Abstract: Seemingly, the history of data protection is a success story culminating in the recognition of data protection as a separate fundamental right in the 2000 EU Charter of Fundamental Rights. This paper assesses the future of the approach taken towards data protection. Using Lessig's typology, the EU Charter should be regarded as a transformative constitution rather than as a codifying constitution. Of these two types, the transformative constitution is clearly the more difficult to realize, since it must act when the constitutional moment is over. Lessig is sceptical about the role of the courts when it comes to realizing such a constitutional project. Today European courts at all levels do take up the task of constitutionalising data protection. This paper discusses the process of constitutionalisation of data protection and its reception by the European Court on Human Rights in Strasbourg and the Court of Justice of the European Communities in Luxembourg.

I. FORMAL OR POLITICAL CONSTITUTIONALISATION

The underlying interests of data protection

It is impossible to summarise data protection in two or three lines. Data protection is a catch-all term for a series of ideas with regard to the processing of personal data (see below). By applying these ideas, governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, the need for government surveillance, applying taxes, etc. In general, data protection does not have a prohibitive nature like criminal law. Data subjects do not own their data. In many cases, they cannot prevent the processing of their data. Under the current state of affairs, data controllers (actors who process personal data) have the right to process data pertaining to others. Hence, data protection is pragmatic; it assumes that private and public actors need to be able to use personal information because this is often necessary for societal reasons. Data protection regulation does not protect us from data processing, but from unlawful and/or disproportionate data processing.

Data protection regulation's real objective is to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details.² This objective seems to be indebted to the central objective of the right of privacy, viz to protect against unjustified

¹ Report on the First Report on the Implementation of the Data Protection Directive 95/46/EC, Committee on the Citizens' Rights and Freedoms, Justice and Home Affairs, European Parliament, Session Document, 24 February 2004 (Final A5-0104/2004), p. 13 http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/ep_report_cappato_04_en.pdf

² P.J. Hustinx, 'Data protection in the European Union', *Privacy & Informatie*, 2005, No. 2, (pp. 62-65), p. 62.

interferences in the personal life. Many scholars therefore hold data protection and privacy to be interchangeable. Data protection is then perceived as a late privacy spin-off. We will come back to the relationship between privacy and data protection below. We would like to underline here that, data protection regulation does a lot more than echoing a privacy right with regard to personal data. Rather, it formulates the conditions under which processing is legitimate. This entails amongst others that data must be processed fairly,³ for specified purposes and, on the basis of the consent of the person concerned or some other legitimate basis laid down by law.⁴ Data protection also prohibits certain processing of personal data, for instance ‘sensitive data’.⁵ A key principle to determine what is legitimate and what is prohibited is the purpose specification principle: data may only be processed when it is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.⁶ Next to these two guidelines regarding legitimacy and unlawful processing, a couple of specific subjective rights are granted to the data subject. These are inter alia the right to be properly informed, the right to have access to one’s own personal data, the right to rectification of data, the right to be protected against the use of automated profiling, the right to swift procedures in court, the right to assistance by Data Protection Authorities (DPAs) competent for a variety of tasks with broad discretionary powers (reporting, monitoring, complaints handling, rule development, enforcement),⁷ a right upon security measures to be implemented by ‘controllers’ and ‘processors’, the right that only relevant data will be gathered and that they will not be disclosed except with consent of data subject or by authority of law.

We see data protection as a growing body of rules and principles that need to be taken into account by the legislator drafting laws, and by ‘controllers’ and ‘processors of personal data’. This process is never over. New rules and principles are called for every time new challenges arise due to new (technological) developments. It is therefore not easy to define the underlying interest of data protection. Just as there are many visions of privacy in literature - from narrow visions (*protection of the intimate sphere* proposed by inter alia Wacks, Inness),⁸ older visions (*the right to be let alone* proposed by Warren & Brandeis or the dignity approach),⁹ newer visions (‘identity’ as proposed by Hildebrandt)¹⁰ over to broader visions (*privacy as freedom and informational self-determination* proposed by inter alia Westin and Gutwirth),¹¹ there are many ‘readings’ possible of the interests underlying data protection and their priority, ranging from autonomy, informational self-determination, balance of powers, informational division of powers, over integrity and dignity, to democracy and pluralism.¹²

³ See Article 5 of the 1981 Convention, Article 6(1)(a) of the 1995 Directive and Article 4(a) Regulation 45/2001

⁴ See Article 5 of the 1981 Convention, Article 4-7 of the 1995 Directive and Article 4(1) (b) Regulation 45/2001. We will come back to these texts below.

⁵ Data protection law includes extra safeguards with regard to the processing of sensitive data or ‘special categories of data’, such as data on ethnicity, gender, sexual life, political opinions or the religion of the person (Article 6 of the 1981 Convention, Article 8 of the 1995 Directive and Article 10 Regulation 45/2001). The special responsibility of the data processor towards sensitive data can be explained by the fact that the information at stake, for example medical data, belongs to the core of a person’s private life. It is exactly this kind of information that individuals generally do not wish to disclose to others.

⁶ See Article 5 of the 1981 Convention, Article 6(1)(b) of the 1995 Directive and Article 4(1)(b) Regulation 45/2001

⁷ See on these DPAs, Article 1 of the Additional Protocol to the 1981 Convention, Article 28 of the 1995 Directive and Article 24 and 41 Regulation 45/2001

⁸ Raymond Wacks, ‘The Poverty of Privacy’, *Law Quarterly Review*, 1980, vol. 96, p. 73 ff.; Julie C. Inness, *Privacy, Intimacy, and Isolation*, Oxford. University Press, 1992.

⁹ Samuel D. Warren & Louis D. Brandeis, ‘The Right to Privacy’, *Harvard L. Rev.* 1890, pp. 195-215; Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser’ *N.Y.U. L. REV.*, 1964, Vol. 39, p. 962 ff..

¹⁰ M. Hildebrandt, M., ‘Privacy and Identity’, in Claes, E., Duff, E., Gutwirth, S. (eds.), *Privacy and the Criminal Law*, Antwerp- Oxford: Intersentia 2006, pp. 43-58.

¹¹ F. Westin, *Privacy and Freedom*, Bodley Head, London, 1967; S. Gutwirth, *Privacy and the information age*, Lanham/Boulder/New York/Oxford, Rowman & Littlefield Publ., 2002, 146p.

¹² E. Brouwer, *Digital Borders and Real Rights*. Nijmegen, Wolf Legal Publishers, 2007, (501p.), p. 170-175; P. De Hert & S. Gutwirth, ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’ in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, p. 61-104; L. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Deventer, Kluwer Law International, 2002, 448p.; L. Bygrave, ‘Regulatory logic of data protection laws’,

Formal constitutionalism and the history of data protection

The history of European data protection is a well-known example of legal creativity and perseverance of some of the visionary in the policy making world, realizing that the right to privacy in Article 8 of the European Convention for the protection of human rights and fundamental freedoms (ECHR), adopted in 1950, needed to be complemented to meet some of the challenges created by emerging technologies in the 1970s.¹³ In the early 1970s the Council of Europe concluded that Article 8 ECHR had a number of limitations in the light of new developments, particularly in the area of information technology: the uncertain scope of private life, the emphasis on protection against interference by public authorities, and the insufficient response to the growing need for a positive and pro-active approach, also dealing with other relevant organisations and interests.¹⁴ As a consequence, the Council of Europe adopted a separate Convention on Data Protection (1981)¹⁵ dealing with data protection as protection of fundamental rights and freedoms of individuals, in particular their right to privacy, with regard to the processing of personal data relating to them. These wordings demonstrate that data protection is both wider and more specific than the protection of privacy. It is wider since it also relates to other fundamental rights and freedoms of individuals, such as equality and due process. It is at the same time more specific, since it only deals with the processing of *personal data*. However, it is broader because it protects all personal data. We will see below that both the Strasbourg Court of Human Rights and the Luxembourg Court of Justice refuse to consider privacy protection to be applicable to all personal data.¹⁶

The Council of Europe Convention was followed by several EU regulatory initiatives:¹⁷ the 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 (Directive 95/46/EC),¹⁸ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector,¹⁹ replaced by Directive 2002/58/EC on privacy and electronic communications of 12 July 2002,²⁰ and 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.²¹ For our purposes, the constitutional recognition of data protection in the EU 2001

February 2007, (2p.), p. 1 (via <http://www.uio.no/studier/emner/jus/jus/JUR5630/v07/undervisningsmateriale/lecture5v07.doc>). Cf. the contribution of Poullet and Rouvroy in this book.

¹³ See in more detail: P. De Hert & S. Gutwirth, 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute for Prospective Technological Studies-Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, p. 125-127. See also Birte Siemen, *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot, 2006. 351 p. See on this excellent study the book review by Cornelia Riehle, *CML Rev.* 2007, pp. 1192-1193

¹⁴ P.J. Hustinx, *l.c.*, p. 62.

¹⁵ Council of Europe, Convention for the Protection of Individuals with regard to automatic processing of personal data, 28 January 1981, ETS No 108. Available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

¹⁶ Whereas data protection covers all personal data, privacy protection understood by the Court only grants privacy protection to certain (uses of) data. Compare ECJ, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauerermann (C-139/01) v Österreichischer Rundfunk*, Judgement of 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01, *European Court reports*, 2003, p. I-04989; §§ 74-75: While the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the European Convention on Human Rights.

¹⁷ See for the rationale of these EU initiatives: P.J. Hustinx, *l.c.*, p. 63.

¹⁸ *O.J.*, No. L 281, 23 November 1995, pp. 31-50

¹⁹ *O.J.*, No L 24, 30 January 1998, pp. 1-8

²⁰ *O.J.*, No L 201, 31 July 2002, pp. 37-47

²¹ *O.J.*, 12 January 2001, L8, pp. 1-22

Charter of Fundamental Rights of the European Union is important.²² In this non-legally binding Charter, a separate right to data protection is recognized next to the right to a private life for the individual. Whereas Article 7 of the Charter faithfully reproduces the wordings of the right to privacy as we know it from the 1950 Human Rights Convention,²³ Article 8 of the Charter focuses on the protection of personal data:

‘Everyone has the right to the protection of their personal data. 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 their data, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority’ (Article 8 EU Charter).

In the ECHR there is no article that comes close this provision. Apparently, something new is happening at constitutional level.²⁴ The Council of Europe’s Convention on Data Protection (ETS No. 108) and the European Community’s Data Protection Directive 95/46 only regard data protection as a facet of the existing fundamental rights such as the right to privacy. Here the constitutional lawmaker goes one step further and provides for an independent fundamental right.

The 2000 Charter was inserted (slightly modified) in the Treaty Establishing a Constitution for Europe signed on October 29, 2004.²⁵ This Constitutional text encountered ratification problems in some Member States and was not formally carried through. Instead, its main provisions were copied in a Reform Treaty for the European Union amending the framework based on the existing Treaties.²⁶ The final text of the treaty, drawn up during the Inter-Governmental Conference (IGC), was approved at the informal European Council in Lisbon on 18 and 19 October 2007. This ‘Treaty of Lisbon’ was signed by the Member States on 13 December 2007,²⁷ and the feeling is that this time it will meet successful ratification.²⁸ Not all of the Constitution’s innovations were taken up in the Reform Treaty, but much of its substance has been maintained, including its provisions regarding human rights. The Treaty opens the way for the Union to seek accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms (the aim of accession is envisaged in the revised Article 6.2 TEU) and it guarantees the enforcement of the Charter of Fundamental Rights of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, ‘which shall have the same legal value as the Treaties’ (revised Article 6.1 TEU).²⁹ Hence, although the text of the Charter is not incorporated into the EU Treaty, it has given a legally binding value for EU institutions and bodies as well as for the Member States as regards the implementation of Union law.³⁰ In addition, the Lisbon Treaty provisions provide for data protection in areas

²² Charter of Fundamental Rights of the European Union of the European Parliament, December 7, 2000, *O.J.*, No. C 364, 2000, p. 1 et seq.

²³ ‘Everyone has the right to respect for his or her private and family life, home and communications’ (Article 7 EU Charter).

²⁴ O. De Schutter, ‘Article II-68 – Protection des données à caractère personnel’, in L. Burgorgue-Larsen, A. Levade and F. Picod (eds.), *Traité établissant une Constitution pour l’Europe: Commentaire article par article*, Brussels, Bruylant, 2005, pp. 122-152.

²⁵ Treaty Establishing a Constitution for Europe, *O.J.*, No. C 310, 16 December 2004, p. 1-474.

²⁶ The new ‘Reform Treaty’ was not meant to be a ‘Constitution’ and would *not* replace the existing treaties, namely the Treaty on European Union (TEU) and the Treaty of the European Community (TEC). It would be just an ‘amending treaty’ consisting of two substantive clauses modifying, respectively, the TEU (which would keep its name) and the TEC, which would instead be called ‘Treaty on the Functioning of the Union’, and the EU would acquire a single legal personality (as foreseen by the Constitutional Treaty).

²⁷ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *O.J.*, No. C 306, 17 December 2007, pp. 1-271.

²⁸ It is up to each country to choose the procedure for ratification, in line with its own national constitution. The target date for ratification set by member governments is 1 January 2009.

²⁹ An adapted version of the Charter was proclaimed on December 12, 2007 in Strasbourg, ahead of the signing of the Treaty of Lisbon containing a slightly modified version of the 2000 EU Charter, to make it resemble the text that was part of the rejected European Constitution.

³⁰ For the exceptions on this made for two Member States, see the Protocol on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, *O.J.*, No. C 306, 17 December 2007, p. 156-157.

such as judicial cooperation in criminal matters and police cooperation,³¹ and for data protection in the area of common foreign and security policy.³²

Rationale

The recognition of a data protection as a fundamental right in the EU legal order has been welcomed for many reasons. First, there were considerations with regard to the legitimacy of the EU data protection framework. From the start, the 1995 Data Protection Directive was based on a double logic: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. The Commission itself conceded that although both objectives are said to be equally important, in legal terms the economic perspective and internal market arguments prevailed.³³ Legislation at EU level was justified because of differences in the way that Member States approached this issue which impeded the free flow of personal data between the Member States.³⁴ Second, the rights-objective was less clear, especially since the Directive contained several business-friendly regulations that were far from inspired by human rights arguments.³⁵ The recognition of a right to data protection in the Charter can be seen as a way to remedy this by adding emphasis to the fundamental rights dimension of the Directive.³⁶

There are other, more convincing reasons to welcome the new right to data protection. Data protection and privacy are not interchangeable. There are important differences between the two in terms of scope, goals and content. As previously mentioned above, data protection explicitly protects values that are not at the core of privacy, such as the requirement of fair processing, consent, legitimacy and non-discrimination.³⁷ The explicit recognition in the new provision of a 'right of access to data that has been collected concerning him or her, and the right to have it rectified' solves legal problems unanswered by the case law of the European Court of Human Rights. Equally, in this case law there are no grounds for a right to have (all)

³¹ See the new Article 16 B, replacing Article 286: 1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 25a of the Treaty on European Union'.

³² See Article 25a of the new TEU: 'In accordance with Article 16 B of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities'.

³³ Commission of the European Communities, *First Report on the implementation of the Data Protection Directive (95/46/EC)*, (COM (2003) 265), Brussels, 15 May 2003, 27p. (via http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf), 3.

³⁴ See also Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security. COM (90) 314 final, 13 September 1990, (via http://aei.pitt.edu/3768/01/000273_1.pdf) (135p.), page 4: '*The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded...*'. As a consequence the legal base of the Directive was Article 100a (now Article 95) of the Treaty.

³⁵ S. Gutwirth, *Privacy and the information age, o.c.*, pp. 91-95.

³⁶ Commission of the European Communities, '*First report*', *o.c.*, p. 3.

³⁷ Take for instance the right not to be discriminated against protected by Article 15 of the Data Protection Directive. According to this article every person has the right 'not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data.' The article refers to automated processing of data 'intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.' The goal is to guarantee everyone's participation in important personal decisions. A dismissal based purely on the data from the company time clock is, as a result, unacceptable. It applies also to the rejection of a jobseeker based on the results of a computerized psycho-technical assessment test or to a computerized job application package. Those decisions have to take professional experience or the result of a job interview into account. The automated test is insufficient and it applies to such sectors as banking and insurance. The EU member states have to enact provisions that allow for the legal challenge of computerized decisions and which guarantee an individual's input in the decision-making procedures. However member states are allowed to grant exemptions on the ban on computerized individual decisions if such a decision '(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

data protection rules controlled and monitored by an independent authority, as is foreseen by the last paragraph of the new provision.³⁸ Furthermore, the Charter extends the protection of personal data to private relations and the private sector.³⁹

The non-interchangeability of privacy and data protection is not merely positivist, it has deeper character. While privacy obviously occupies a central place in data protection law, the characterisation of data protection law as solely or even essentially concerned with safeguarding privacy is misleading.⁴⁰ Data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualisations of privacy.⁴¹ Few direct manifestations of intimacy-oriented conceptions of privacy are to be found in the provisions of data protection laws and, even broader privacy concepts are not of a nature to explain data protection principles such as purpose limitation, data quality or security.⁴² Finally, we believe that the recognition of a separate right to data protection, next to privacy, to be more respectful to the European constitutional history. Just as there are different constitutional footings for privacy protection in the United States, the EU and Canada,⁴³ there are and remain distinctive constitutional traditions within the European Union that influence the way privacy and data protection are interpreted. Contrary to countries like Belgium and the Netherlands that have linked data protection from the start to privacy, countries like France and Germany, lacking an explicit right to privacy in their constitution, have searched and found other legal anchors for the recognition of data protection rights. French data protection was based on the right to liberty, whereas German data protection was based on the right to the recognition of human dignity. All these approaches, which are different to the US tradition that seems to build its data protection principles upon public law principles such as fair information practices⁴⁴, cannot be considered to be identical and might explain differences in data protection between the EU Member States.

Life is easier with transformative constitutions

How innovative was the Charter? At a national level, the right to data protection was only directly or indirectly protected by the constitution in a few countries.⁴⁵ The 1976 Portuguese Constitution foresaw a right of knowledge regarding the automated processing of personal data and a ban on the use of personal ID numbers. Since its revision in 1983, the Dutch Constitution provides the legislator with the task of regulating the use of information technology and the protection of personal life.⁴⁶ Section 18.4 of the Spanish 1978 Constitution

³⁸ Article 13 ECHR (right to an effective legal remedy) is not an independent right. The European Court refuses to consider issues under this provision, when there is no violation of another right of the ECHR.

³⁹ Cf. Y. Poullet, 'Pour une justification des articles 25 et 26 en matière de flux transfrontières et de protection des données' in M. Cools, C. Eliaerts, S. Gutwirth, T. Joris & B. Spruyt (eds), *Ceci n'est pas un juriste ... mais un ami. Liber Amicorum Bart De Schutter*, Brussels, VUBPress, 2003, p. 278.

⁴⁰ L. Bygrave, 'The Place Of Privacy In Data Protection Law', *University of NSW Law Journal*, 2001, (6p.), sub § 18 (via <http://www.austlii.edu.au/journals/UNSWLJ/2001/6.html>)

⁴¹ *Ibid.*

⁴² *Ibid.* § 15; E. Brouwer, *o.c.*, p. 205; P. De Hert & S. Gutwirth, 'Making sense of privacy and data protection', *l.c.*, p. 111 ff.

⁴³ See Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', *University of Ottawa Law & Technology Journal*, Vol. 2, No. 2, pp. 357-395, 2005 (also available at SSRN: <http://ssrn.com/abstract=894079>). The EU and Canada centrally supervise the private sector's use of personal data, whereas the US regulation of the private sector is minimal Avner Levin and Mary Jo Nicholson look behind these and other differences in regulation to be found in the European Union (EU), the United States (US) and Canada, and hold that they emanate from distinct conceptual bases for privacy in each jurisdiction: In the US, privacy protection is essentially liberty protection, i.e. protection from government. For Europeans, privacy protects dignity or their public image. In Canada, privacy protection is focused on individual autonomy through personal control of information.

⁴⁴ P. Blok, Botsende rechtsculturen bij transatlantisch gegevensverkeer, *Nederlands Juristenblad (NJB)*, 2001, pp. 1607-1612

⁴⁵ E. Brouwer, *o.c.*, p. 167.

⁴⁶ Article 10 of the Dutch Constitution: '(1) Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament. (2) Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data. (3) Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament' (http://www.servat.unibe.ch/law/icl/nl00000_.html).

gives a similar mandate, but only in so far that data is linked to exercising the right to honour and privacy.⁴⁷ Most European constitutions do not speak about protecting personal data. Therefore it is very interesting to note how few arguments were advanced to incorporate a separate right to data protection in the Charter. In the Explanatory report to the Charter no reasons are given, there is only a reference to the 1995 Directive and the 108 Council of Europe Convention.⁴⁸ According to the Commission the incorporation of the right to data protection, gives added emphasis to the fundamental right dimension of EC Directive 95/46 on data protection.⁴⁹ Indeed the writing process of the Charter was unusual, since the draft was prepared by an ad-hoc Convention body comprising representatives from the European Parliament, national parliaments, the European Commission, governments and some observers.⁵⁰ During the preparation of the Draft the parties did not experience many difficulties. Part of the preparatory work was done by expert committees. An explanation for the success of the Convention could be that incorporating the existing rights into one document without having to invent new rights was seen as merely a technical exercise. Working Party 29 used a very technical approach in its 1999 initiative to include data protection in the fundamental rights of Europe. This ‘would make such protection a legal requirement throughout the Union and reflect its increasing importance in the information society’.⁵¹ There would be no further detailed analysis of the existing constitutions of the Member States, no reference to the case law of the Strasbourg Court of Human Rights. Nevertheless, because of its recognition in the Charter one can claim that data protection became part of Western *constitutionalism*. One even could defend the view that data protection today is part of the European *Constitution*⁵², regardless of the name we give to primary EU treaty law, and that it has achieved an independent fundamental status next to the right to privacy.⁵³

In *Code and other laws of cyberspace* Lawrence Lessig distinguishes between two types of constitutions, one he calls codifying and the other transformative. Codifying constitutions preserve essential tenets of the constitutional or legal culture in which they are enacted and aim at protecting them against changes in the future, whereas transformative constitutions or transformative amendments to existing constitutions aim at changing essential aspects of the constitutional or legal culture in which they are enacted.⁵⁴ For Lessig, the US Constitution of 1789 qualifies as a transformative constitution, since it initiated a new form of government and gave birth to a nation, whereas the US Constitution of 1791—the Bill of Rights—

⁴⁷ Section 18: ‘1. The right to honour, to personal and family privacy and to the own image is guaranteed. 2. The home is inviolable. No entry or search may be made without the consent of the householder or a legal warrant, except in cases of a flagrant delict. 3. Secrecy of communications is guaranteed, particularly regarding postal, telegraphic and telephonic communications, except in the event of a court order. 4. The law shall restrict the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights’ (Source: http://en.wikisource.org/wiki/Spanish_Constitution_of_1978/Part_I). See however the decision of November 30, 2000 in which the Spanish Constitutional Court recognised a fundamental right to data protection which differs from the right to privacy set out under Article 18 of the Constitution. See ‘Spain. Constitutional Challenge to Data Protection Law’, *World Data Protection Report*, 2001, p. 7.

⁴⁸ Council of the European Union, *Charter of Fundamental Rights of the European Union. Explanations relating to the complete text of the Charter. December 2000*, Luxembourg: Office for Official Publications of the European Communities, 2001, (77p.), p. 26

⁴⁹ European Commission, *First Report on the implementation of the Data Protection Directive*, 15 May 2003. o.c.

⁵⁰ The Cologne European Council (3/4 June 1999) entrusted the task of drafting the Charter to a Convention. The Convention held its constituent meeting in December 1999 and adopted the draft on 2 October 2000. Its composition was established at the European Council meeting in Tampere in October 1999. See on the composition: http://www.europarl.europa.eu/charter/composition_en.htm

⁵¹ Working Party on the Protection of Individuals with Regard to the Processing of Personal Data Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, September 1999, 5143 /99/ENWP 26, 3p. (available via http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp26en.pdf)

⁵² When does a treaty become a constitution? ‘A treaty as an interstate act may give rise to rights to individuals but this is a by-product of the settlement of relations between states. A constitution is the embodiment of the compromise of rights and duties between the people and those exercising authority. Giving precision to rights of individuals is central to constitution making’ (Elsbeth Guild, ‘Citizens, Immigrants, Terrorists and Others’, in A Ward and S Peers (eds) *The EU Charter of Fundamental Rights: Politics, Law and Policy* Hart, Oxford, 2004, (pp. 321 – 246), p. 322.

⁵³ See B. Siemen, o.c., par. 3.D.; H.K. Kranenborg, *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie*, Deventer, Kluwer, 2007, (351p.), pp. 172-173.

⁵⁴ L. Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, p. 213.

qualifies as a codifying constitution, entrenching certain values against future change. The Civil War amendments were transformative, since they aimed to break the American tradition of inequality and replace it with a tradition and practice of equality.⁵⁵

There may be no doubt about the codifying character of the EU Charter, preserving a European human rights heritage and being the result of a merely ‘technical’ exercise. However, the transformative side of the Charter is less well-known. This is a side which is not only illustrated by the right to data protection, but by many more examples,⁵⁶ and indeed the codification of human dignity taken from the German constitution as the mother right of the EU Charter, proudly occupying the royal throne of the Charter in its first article, but absent as a concept in almost all Member State constitutions, except for the German one.⁵⁷ Lessig observes that of the two constitutional options, the transformative constitution is clearly the most difficult to realise. A codifying regime at least has inertia on its side; a transformative regime must fight.⁵⁸ Of course this implies not much more than the old wisdom about the difficulty to enforce rights and duties that are not properly internalised by the legal subjects. The failure of some recent Canadian copyright initiatives with regard to the Internet should be understood in this perspective: attempts to use copyright as a tool to prohibit certain use of information failed for two reasons: it deviates from the original intent of copyright (the regulation of the interaction between professional actors responsible for the creation, publication, production and dissemination of works of the mind) and it is not rooted in a moral imperative, but clashes with strong social norms that have developed specifically because of the informal, intuitive and global nature of the Internet.⁵⁹ End-users do not consider themselves as pirates and do not act with the intent of commercial gain. It is therefore no surprise, one author notes, to observe that the Canadian Supreme Court did not uphold the new copyright regulation.⁶⁰

Hence, new legal and constitutional values are put to test and if the courts do not feel certain about them, they might resort to more familiar old values. Lessig sees this as a general problem in Cyberworld, where judges have to make judgments that do not seem to flow plainly or obviously from a legal text.⁶¹ This brings us to our central question. How is data protection as a newly recognised constitutional value received in the field, i.e. by the courts? Subsequently, we will deal with the following lines of analysis: the reception of data protection by the European Court on Human Rights in Strasbourg (ECtHR) and the reception of data protection by the European Court of Justice in Luxembourg (ECJ). The reception of data protection by national courts also needs our attention, but we will deal with this issue elsewhere.

⁵⁵ L. Lessig, *o.c.*, p. 214.

⁵⁶ The EU Charter incorporates most of the content of the ECHR, but purposely proclaims additional rights not contained in the European Human Rights Convention of which data protection is only one example. Other examples are bioethics, the right to good administration, a general prohibition to outlaw discrimination on the grounds of gender, race and colour and certain social rights.

⁵⁷ The right to dignity is also mentioned in Section 10.1 of the Spanish 1978 Constitution but it is only one source of constitutionalism amongst others. Article 23 of the 1994 Belgian Constitution equally protects human dignity but this is tied to certain economic, social and cultural rights. See http://en.wikisource.org/wiki/Constitution_of_Belgium

⁵⁸ ‘The codifying regime has a moment of self-affirmation; the transformative regime is haunted with self-doubt, and vulnerable to undermining by targeted opposition. Constitutional moments die, and when they do, the institutions charged with enforcing their commands, such as courts, face increasing political resistance. Flashes of enlightenment notwithstanding, the people retain or go back to their old ways, and courts find it hard to resist’ (L. Lessig, *o.c.*, 214).

⁵⁹ Daniel J. Gervais, ‘The Purpose of Copyright Law in Canada’, *University of Ottawa Law & Technology Journal*, 2005, Vol. 2, pp. 315-358. ‘While Internet users apparently do not agree that their file-sharing behaviour is morally wrong, a view supported historically in many cultures where stealing a work of the mind meant plagiarizing or using without proper attribution, their cyberspace behaviour has shaped a new social norm of creating multiple links, by email, in chat groups, blogs or other Internet tools, with people with whom they share certain interests. This is reinforced by hyperlinks that allow users to ‘intuitively’ follow their train of thought. That requires access, not roadblocks. In a world where millions of Internet users are paying for high-speed to avoid having to wait to access material, a refusal to grant access because of a prohibition-based copyright is unlikely to be well received and accepted’ (Daniel J. Gervais, *l.c.*, 335)

⁶⁰ *Ibid.*

⁶¹ L. Lessig, *o.c.*, 215.

II. THE MATERIAL CONSTITUTIONALISATION OF DATA PROTECTION

II.1. Data protection tested in Strasbourg

A right to autonomy under the scope of Article 8 ECHR?

The 1950 European Convention is a very straightforward human rights declaration carefully avoiding metaphysical references. In the Convention there is, for instance, no general recognition of the right to liberty, neither of the right to the protection of human dignity, nor of the right to autonomy or the right to self-determination. Avoiding these weighty references is not unwise from a comparative constitutional perspective. We briefly mentioned above that privacy and data protection in the European Member States are differently rooted. Hence, for instance, German case law developed a right of informational self-determination (meaning the capacity of the individual to determine in principle the disclosure and use of his/her personal data) on basis of the concepts of dignity and self-determination in the German Constitution.⁶² In the French Constitution, where these concepts are absent, data protection was based on the broader notion of liberty,⁶³ whereas the Dutch and Belgian Constitutions refer to privacy as the source of data protection.

For the richness of European diversity it is a good thing that the ECHR avoids any choice or prioritising of these higher values. It can however be questioned whether human rights application and interpretation is always feasible without referring to these core ethical values. We doubt it. As a result it did not come as a surprise to us that the right to autonomy appeared in the Convention language concerning Article 8, notably in *Pretty v. United Kingdom* (2002). The question was put before the Court whether the right to private life encapsulated a right to die with assistance, for persons paralysed and suffering from a degenerative and incurable illness. *Pretty* alleged that the refusal of the Director of Public Prosecutions to grant an immunity from prosecution to her husband if he assisted her in committing suicide, and the prohibition in domestic law on assisting suicide infringed her rights under Articles 2, 3, 8, 9 and 14 of the Convention. The claim was not recognized, but paragraph 61 of the Judgement contains a very relevant and broad recognition of the principle of personal autonomy:

‘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. Switzerland*, Commission’s report, op. cit., § 47; *Friedl v. Austria*, *Series A* no. 305-B, Commission’s report, § 45). Though no previous

⁶² Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65.

⁶³ As a consequence Article 1 of the 1978 French Data Protection law states that information technology should not infringe upon human rights, including the right to privacy and individual or public liberties.

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’.

We do not think that conceptually all is clear,⁶⁴ but the ruling of the Court shows that the principle of personal autonomy has gained considerable importance within the right of privacy. Whether Article 8 ECHR also entails a right of determination, including informational self-determination, remains unanswered at this point. In *Pretty* the Court leaves this question deliberately open, but we will see that the latest judgments of the Court reveal a tendency in this direction.⁶⁵

The broad scope of Article 8 ECHR

The role of the European Court on Human Rights (and the role of the former European Commission for Human Rights) can be described as twofold, being both a self-contained system of human rights protection and the provider for guidelines for the ECJ for concretising the fundamental rights of the European Community.⁶⁶ The case law of the European Court is traditionally hailed as a powerful demonstration of the strength of the 1950 Convention on Human Rights.⁶⁷ Although the Convention does not evoke modern means of communication, the Court, applying a ‘dynamic and broad’ interpretation of the Convention, has successively brought telephone conversations,⁶⁸ telephone numbers,⁶⁹ computers,⁷⁰ video-surveillance,⁷¹ voice-recording,⁷² and Internet and e-mail⁷³ under the scope of Article 8.⁷⁴ The ease of this ‘method’ or approach is remarkable. Often no more than one paragraph is needed, for instance in *Copland* where the Court ruled that according to its Court's case law, ‘telephone calls from business premises are prima facie covered by the notions of ‘private life’ and ‘correspondence’ for the purposes of Article 8 § 1. It follows *logically* that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage’.⁷⁵

⁶⁴ In *Pretty* autonomy is considered a ‘principle’ and physical and social identity are issues of which ‘aspects’ are sometimes protected by the right to private life. In their joint dissenting opinion to *Odièvre v. France* judges Wildhaber, Bratza, Bonello, Loucaides, Cabral Barreto, Tulkens and Pellonpää consider autonomy and identity to be ‘rights’: ‘We are firmly of the opinion that the right to an identity, which is an essential condition of the right to autonomy (see ECtHR, *Pretty v. the United Kingdom*, Application no. 2346/02, Judgment of 29 April 2002 § 61, *ECHR* 2002-III) and development (see ECtHR, *Bensaid v. the United Kingdom*, Application no. 44599/98, Judgment of 6 February 2001, § 47, *ECHR* 2001-I), is within the inner core of the right to respect for one's private life’ (par. 11 of the Opinion).

⁶⁵ Compare B. Siemen, *o.c.*, pp. 76-78.

⁶⁶ C. Riehle, ‘Book review’ of B. Siemen, *C.M.L.J.*, 2007, p. 1193-1195.

⁶⁷ Case law of Strasbourg is available <http://www.echr.coe.int/echr> and can easily be consulted using the ‘Application Number’. When the Application Number is not mentioned on that site a ‘paper’ source is given.

⁶⁸ ECtHR, *Klass v. Germany*, Application no. 5029/71, Judgment of 6 September 1978, § 41; ECtHR, *Amann v. Switzerland* [GC], Appl. no. 27798/95, Judgment of 16 February 2000, § 44; ECtHR, *Halford v. United Kingdom*, judgment of 25 June 1997, *Reports*, 1997-III, p. 1016, § 44.

⁶⁹ ECtHR, *Malone v. United Kingdom*, Application no. 8691/79, Judgment of 2 August 1984, § 84; ECtHR, *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, § 42; ECtHR, *Copland v. the United Kingdom*, no. 62617/00, Judgment of 3 April 2007, § 43.

⁷⁰ ECtHR, *Leander v. Sweden*, Application no. 9248/81, Judgment of 26 March 1987, § 48; ECtHR, *Amann v. Switzerland*, § 65; ECtHR, *Rotaru v. Romania*, Application no. 28341/95 judgment of 4 May 2000, § 42-43.

⁷¹ ECtHR, *Peck v. the United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, §§ 57-63; ECtHR, *Perry v. the United Kingdom*, Application no. 63737/00, Judgment of 17 July 2003, § 40.

⁷² ECtHR, *P.G. and J.H. v. the United Kingdom*, §§ 59-60.

⁷³ ECtHR, *Copland v. the United Kingdom*, § 41.

⁷⁴ Article 8.1. ECHR states that: ‘Everyone has the right to respect for his private and family life, his home and his correspondence’. For a detailed analysis of the Article 8 ECHR case law, see P. De Hert, *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woonst en communicatie* [Article 8 ECHR and the Law in Belgium. Protection of Privacy, House, Family and Correspondence], Gent, Myn Breesch Uitgeverij, 1998, 367p. P. De Hert, ‘Artikel 8 EVRM. Recht op privacy’ [Article 8 of the Convention on Human Rights. The Right to Privacy] in VANDE LANOTTE, J. & HAECK, Y. (eds.), *Handboek EVRM. Deel 2 Artikelsgewijze Commentaar*, Antwerp-Oxford, Intersentia, 2004, 705-788; P. De Hert & A. Hoefmans, ‘Het arrest *Copland* in het kader van de verdieping van de Europese rechtspraak op het gebied van privacybescherming’, *European Human Rights Cases (EHRC)*, 13 June 2007, Vol. 8, No. 6, pp. 664-674

⁷⁵ ECtHR, *Copland v. the United Kingdom*, § 41, with ref. to ECtHR, *Halford v. United Kingdom*, § 44 and ECtHR, *Amann v. Switzerland*, § 43 (italics added).

In many of these expansive judgements, the Court applies a broad definition of the notion of private life in Article 8 ECHR, extending it far beyond the walls of the private house and the intimate sphere. In this view ‘private life’ embraces development of interpersonal relationships,⁷⁶ and protects not only the domestic sphere, but also (data relating to) certain facts occurred in the public sphere.⁷⁷ The Court has even gone so far as to recognise privacy protection to firms and business activities,⁷⁸ which is a non-mandatory feature of data protection regulation (which optionally allows Members States to recognise data protection rights not only to natural persons but also to legal persons).

With respect to Article 8 ECRM and other rights enshrined in the Convention, the Court recognises positive state duties (making certain rights possible) next to negative state duties (not to infringe certain rights). The existence of these positive duties has allowed the Court to construct certain data protection rights, such as the right to access to data, compulsory in most cases under Article 8 ECHR (see below). Based on these notions of positive state duties, states can be held responsible for privacy infringements caused by private actors, such as firms and newspapers or by public authorities acting in roles that can also be assumed by private actors, for instance the role of employer or the press.⁷⁹ Although these private actors cannot be sued directly before the Strasbourg Court, this case law of the Court can be invoked by interested parties in a national court.⁸⁰

Several aspects of data protection under the scope of Article 8 ECHR

The Strasbourg organs also have brought several issues under the scope of Article 8 ECHR that are more specifically related to or characteristic for data protection.⁸¹ In order to bring new technologies under the Convention (supra), the Court has made skilful use of the co-presence in Article 8 ECHR of both the right to protection of private life *and* correspondence, often leaving open which one of the two needs to be regarded as the primary right.⁸² Increasingly, it uses insights and principles taken from data protection regulation to consider

⁷⁶ ECtHR, *Niemietz v. Germany*, Application no. 13710/88, Judgement of 16 December 1992, § 29: ‘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. There appears, furthermore, to be no reason of principle why this understanding of the notion of ‘private life’ should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual’s activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time’.

⁷⁷ ECtHR, *Peck v. the United Kingdom*, §§ 57-63.

⁷⁸ ECtHR, *Société Colas Est and others v. France*, Application no. 37971/97, Judgement of 16 April 2002, § 40: ‘ Building on its dynamic interpretation of the Convention, the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company’s registered office, branches or other business premises (see, *mutatis mutandis*, *Niemietz*, cited above, p. 34, § 30)’.

⁷⁹ See on the role of the press and the conflict with the right to privacy, ECtHR, *Von Hannover v Germany*, Application no. 59320/00, Judgement of 24 June 2004 and 28 July 2005.

⁸⁰ See for a discussion of the applicability of Article 8 ECHR: B. Siemen, *o.c.*, pp. 177-204 (direct third-party applicability is not afforded by Article 8 ECHR; indirect third-party applicability against interferences by private persons is set through the laws).

⁸¹ For a detailed discussion: E. Brouwer, *o.c.*, 133-144; P. De Hert, ‘Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955-1997’ [Human Rights and Data Protection. European Case law 1995-1997], in *Jaarboek ICM 1997*, Antwerp, Maklu, 1998, p. 40-96; O. De Schutter, ‘Vie privée et protection de l’individu vis-à-vis des traitements de données à caractère personnel’, obs. sous Cour eur. D.H., arrêt Rotaru c. Roumanie du 4 mai 2000, *Revue trimestrielle des droits de l’homme*, n°45, 2001, pp. 137-183.

⁸² See on the protection of telephone numbers in *Malone*: ‘As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8)’ (§ 84).

issues raised by modern technologies.⁸³ Already in the 1980s it was recalled on several occasions that data protection is an issue which falls within the scope of Article 8.⁸⁴ But particularly since the mid-1980s reference to the data protection framework and the acknowledgment in one way or another of its principles has been more explicit. The Court has associated its broad interpretation of the term ‘private life’ Article 8 ECHR with the equally broad notion of ‘personal data’ in data protection regulation.⁸⁵ In several cases the Court added that information (about persons) belonging in the public domain may fall within the scope of Article 8, once it is systematically stored.⁸⁶

Also the Court recognised the right of individuals to have control, to a certain extent, of the use and registration of their personal information (informational self-determination). In this respect the Court has considered and recognised access claims to personal files,⁸⁷ claims regarding deletion of personal data from public files,⁸⁸ claims from transsexuals for the right to have their ‘official sexual data’ corrected.⁸⁹ Moreover, the Court has insisted on the need for an independent supervisory authority as a mechanism for the protection the rule of law and to prevent the abuse of power, especially in the case of secret surveillance systems.⁹⁰ In other cases the Court demanded access to an independent mechanism, where specific sensitive data were at stake or where the case concerned a claim to access to such data.⁹¹ In *Peck*, in *Perry* and in *P.G. and J.H.* the Court acknowledged the basic idea behind the fundamental principle of purpose limitation in data protection, viz that personal data cannot be used beyond normally foreseeable use.⁹² In *Amann* and *Segerstedt-Wiberg* the Court demanded that governmental authorities only collect data that is relevant, and based on concrete suspicions.⁹³ Finally, in the *Rotaru v. Romania* judgement of 4 May 2000 the Court acknowledged the right

⁸³ See for instance ECtHR, *Copland v. the United Kingdom*, § 43: ‘The Court recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an ‘integral element of the communications made by telephone’ (see *Malone v. the United Kingdom*, judgement of 2 August 1984, Series A no. 82, § 84). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1 (...). Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings’ (italics added). See also ECtHR; *Amann v. Switzerland*, § 65 and ECtHR, *Rotaru v. Romania*, § 42-43 where the *Leander* acquies about storing personal data as falling under the scope of Article 8 ECHR is complemented with a brief discussion of the Council of Europe’s Data Protection Convention of 28 January 1981 to support the argument that even stored data on business contacts should be considered under the light of Article 8 ECHR. See finally the reference to the 1981 Data Protection Convention in ECtHR, *P.G. and J.H. v. the United Kingdom*, § 57 to strengthen the argument that collection of public data by secret services is also a reason of concern from a human rights perspective.

⁸⁴ For instance: ECommissionHR, *Lundvall v. Sweden*, 11 December 1985, case 10473/83, D.R., Vol. 45, 130. See also: ECtHR; *Amann v. Switzerland*, § 65; ECtHR, *Rotaru v. Romania*, Application no. 28341/95 judgement of 4 May 2000, §§ 42-43; ECtHR, *P.G. and J.H. v. the United Kingdom*, § 57.

⁸⁵ ECtHR, *Rotaru v. Romania*, § 43: ‘The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe’s Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is ‘to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him’ (Article 1), such personal data being defined in Article 2 as ‘any information relating to an identified or identifiable individual’.

⁸⁶ ECtHR; *Amann v. Switzerland*, § 65 ; ECtHR, *Rotaru v. Romania*, §§ 43-44; ECtHR, *P.G. and J.H. v. the United Kingdom*, § 57-58; ECtHR, *Segerstedt-Wiberg and others v. Sweden*, Application no. 62332/00, Judgement of 6 June 2006, § 72. See E. Brouwer, *o.c.*, 133 & 137

⁸⁷ ECtHR, *Gaskin v. the United Kingdom*, Application no. 10454/83, Judgement of 7 July 1989; ECtHR, *Antony and Margaret McMichael v. United Kingdom*, Application no. 16424/90, judgement of 24 February 1995. ECtHR, *Guerra v Italy*, Judgement of 19 February 1998, Reports, 1998-I; ECtHR, *McGinley & Egan v. United Kingdom*, Applications nos. 21825/93 and 23414/94, Judgement of 28 January 2000.

⁸⁸ ECtHR, *Leander v. Sweden*, Application no. 9248/81, Judgement of 26 March 1987; ECtHR, *Segerstedt-Wiberg and others v. Sweden*, Application no. 62332/00, Judgement of 6 June 2006.

⁸⁹ ECtHR, *Rees v UK*, Judgement of 25 October 1986 Series A, No. 106; ECtHR, *Cossey v UK*, Judgement of 27 September 1990, Series A, No. 184; ECtHR, *B v France*, Judgement of 25 March 1992 Series A, No. 232-C; ECtHR, *Christine Goodwin v. the United Kingdom*, Application no. 28957/95, Judgement of 11 July 2002

⁹⁰ ECtHR, *Klass v. Germany*, § 55; ECtHR, *Leander v. Sweden*, §§ 65-67; ECtHR, *Rotaru v. Romania*, §§ 59-60. See in detail: E. Brouwer, *o.c.*, 143-144.

⁹¹ ECtHR, *Gaskin v. the United Kingdom*, Application no. 10454/83, Judgement of 7 July 1989; ECtHR, *Z. v Finland*, Application no. 22009/93, Judgement of 25 February 1997.

⁹² 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. More in detail: E. Brouwer, *o.c.*, 138-139.

⁹³ This requirement is part of the notion of ‘foreseeable’, one of the conditions that the Court attaches to the phrase ‘in accordance with the law’ contained in Article 8.2. See ECtHR; *Amann v. Switzerland*, § 61 and § 75 ff.; ECtHR, *Segerstedt-Wiberg v. Sweden*, § 79. More in detail: E. Brouwer, *o.c.*, 136-137.

to individuals to financial redress for damages based on a breach of Article 8 caused by the data processing activities of public authorities.⁹⁴

Strasbourg criteria for excessive, unnecessary or and unjustified collection of processing of data

What the Court does in its case law is to establish criteria that allow for an assessment of data protection under the ECHR. In terms of data protection regulation, these criteria are not new but is useful to see the Court embracing them on the fundamental rights level of the ECHR. These criteria are however, so we contend, of the uttermost importance, also for data protection, when they regard the interpretation of broad but essential notions such as 'excessive', 'unnecessary' or 'unjustified' collection of processing of data.⁹⁵ These notions reappear in Article 6(1)(c) and Article 7(c) or (e) of the EU 1995 Data Protection Directive 95/46.

The question whether a certain practice is 'necessary in a democratic society' is however seldom answered by the Court, which usually first addresses the question 'is there a legal basis in law for the privacy infringing action'. When it finds a breach of this legality requirement, it does not verify the other requirements.⁹⁶ This explains why in practice we find only a few rulings on the necessity requirement compared to the amount of rulings on the legality requirement. But there is more. We see not only a tendency to limit the analysis to the legality requirement but also a tendency to expand the analysis of the legality requirement by taking into account more and more human rights issues ('foreseeability', 'accessibility', 'protection against abuse', etc.).

Whatever the wisdom might be of this approach,⁹⁷ we need to realise that checking on the legality requirement is a fundamentally different matter from checking on the requirement 'necessary in a democratic society'.⁹⁸ Only the latter requirement deals with the political question whether (processing) power should be limited, stopped or prohibited or, in other words, whether 'opacity' of the individual must be protected.⁹⁹ Even if a restriction of privacy is foreseen by law and serves one of the legitimate objectives summed up in Article 8 § 2 ECHR, this restriction must still be 'necessary in a democratic society' and should not reach further than that. This condition inevitably implies an ultimate balancing of interests, a value judgement and/or a substantial choice, which cannot be found in an exegetic reading of the

⁹⁴ ECtHR, *Rotaru v. Romania*, § 83.

⁹⁵ We borrow from P. De Hert, 'Strafrecht en privacy. Op zoek naar een tweede adem' [Criminal Law and Privacy. Searching for a New Breath], *Rechtshulp. Maandblad voor de sociale praktijk*, 2003/10, 41-54. We recall that Article 8 ECHR does not formulate privacy as an absolute right. Exceptions are made possible in the second paragraph of the provision, but the drafters of the Convention took care to provide safeguards against possible abuse of the right to formulate exceptions. Therefore, if any exception to the protection of data privacy is adopted respect has to be given to the conditions laid down in Article 8.2 ECHR, that is, any invasion of privacy for a legitimate reason (for purposes of criminal investigation, usually the prevention of crime) must be adopted 'in accordance with the law' and when 'necessary in a democratic society'. Those requisites are cumulative. Article 8.2. ECHR 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.'

⁹⁶ The Convention organs treat the requirements of Article 8.2 ECHR as successive hurdles. This means that where they find that a measure complained of is not 'in accordance with the law', then they do not proceed to examine whether the measure satisfies the requirement of 'necessity in a democratic society'. See for instance ECtHR, *P.G. and J.H.*, § 38. 'As there was no domestic law regulating the use of covert listening devices at the relevant time (...), the interference in this case was not 'in accordance with the law' as required by Article 8 § 2 of the Convention, and there has therefore been a violation of Article 8 in this regard. In the light of this conclusion, the Court is not required to determine whether the interference was, at the same time, 'necessary in a democratic society' for one of the aims enumerated in paragraph 2 of Article 8.'

⁹⁷ Our argument needs to take into account the small implications that judges make. Implying something without really saying it. Judges refrain from politically tainted arguments and prefer to play safe. In *Perry* the judges found a breach of the requirement 'in accordance with the law' and an analysis of the necessity requirement is therefore not made (§ 47-49), but one can find throughout the first analysis sense the message of the Court that would it have done the second analysis, it would have applied a strict proportionality test (§ 41).

⁹⁸ About this condition see K. Rimanque, 'Noodzakelijkheid in een democratische samenleving -een begrenzing van beperkingen aan grondrechten', in *Liber Amicorum Frédéric Dumon*, Antwerp, Kluwer Rechtswetenschappen, 1983, deel II, 1220.

⁹⁹ See on the notion of opacity: P. De Hert & S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, p. 61-104

text, or in a strict application of logical rules.¹⁰⁰ Such a balancing of interests, which takes the weight of fundamental rights and freedoms duly into account, is essential.¹⁰¹ It allows for the exercise of the political function of human rights. Behind the requirement ‘necessary in a democratic society’ lies the true constitutional question with regard to law enforcement and privacy: is there a justifiable necessity for (processing) actors to infringe the privacy right and to process data?

Even in cases when the necessity requirement is met, one cannot but feel some discontent. To believe most authors, the Court, when checking on the requirement of necessity, common to Article 8, 9, 10 and 11 ECHR, applies two criteria, namely the ‘pressing social need’ and the question if the interference can be considered ‘proportionate to the legitimate aim pursued’. It would be a good thing for human freedom if the Court would really just do that, since these criteria, especially the criteria of ‘pressing social need’, put a heavy burden on state actions that are infringing on the rights contained in Article 8, 9, 10 and 11 ECHR.¹⁰² However a closer look at the case law reveals that these criteria are only applied in specific cases, often with regard to Article 10 ECHR, but seldom in cases with regard to Article 8 ECHR where the Court, as a rule, seems less inclined to put a heavy burden on the acting state.¹⁰³ Very seldom the two criteria appear in Article 8 ECHR cases and often the ‘pressing social need’ criteria is omitted in the reasoning of the Court.¹⁰⁴ Often the requirement of ‘necessity’ is brought back to the question of proportionality, in some cases supplemented by the requirement that the reasons for the interference are relevant and sufficient.¹⁰⁵ What is ‘proportionate’ will depend on the circumstances. According to M. Delmas-Marty, in determining proportionality the Court particularly takes into account the nature of the measure taken (its reach, whether it is general or absolute, its adverse consequences, the scope for abuse of the measure), whether the state concerned could have taken other measures or implemented them in a less drastic way, the status of the persons involved whose rights can legitimately be subject to greater limitation (e.g. prisoners) and finally, whether there are any safeguards which can compensate for the infringement of rights which a measure can create.¹⁰⁶ Applied to data protection issues this means that the Court’s proportionality assessment varies according to the gravity of the interference; the sensitivity of the

¹⁰⁰ K. Rimanque, *l.c.*, 1229.

¹⁰¹ Cf. S. Gutwirth, ‘De toepassing van het finaliteitbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens’ [The application of the purpose specification principle in the Belgian data protection act of 8 December 1992], *Tijdschrift voor Privaatrecht*, 4/1993, 1409-1477.

¹⁰² In the context of Article 10 ECHR (freedom of expression) the Court has observed that ‘necessary ... is not synonymous with *indispensable*, neither has it the flexibility of such expressions as *admissible*, *ordinary*, *useful*, *reasonable* or *desirable*, but that it implies a *pressing social need*’ (ECtHR, *Handyside v. United Kingdom*, Judgement of 7 December 1976, *Series A*, No. 24, § 48).

¹⁰³ P. De Hert & S. Gutwirth, ‘Grondrechten: vrijplaatsen voor het strafrecht? Dworkin’s Amerikaanse trumpsmetafoor getoetst aan de hedendaagse Europese mensenrechten’ (Human Rights as Asylums for Criminal Law. An assessment of Dworkin’s Theory on Human Rights) in R.H. Haveman & H.C. Wiersinga (eds.), *Langs de randen van het strafrecht*, Nijmegen, Wolf Legal Publishers, 2005, p. 141-176; P. De Hert, ‘Balancing security and liberty within the European human rights framework. A critical reading of the Court’s case law in the light of surveillance and criminal law enforcement strategies after 9/11’, *Utrecht Law Review*, 2005, Vol. 1, No. 1, 68-96. See: <http://www.utrechtlawreview.org/>

¹⁰⁴ Only in rare cases such as in *Peck* one finds some word games referring to the semantic exercise in the context of Article 10 discussed above. See the use of the term ‘pressing social need’ in the following quote: ‘In such circumstances, the Court considered it clear that, even assuming that the essential complaints of *Smith and Grady* before this Court were before and considered by the domestic courts, the threshold at which those domestic courts could find the impugned policy to be irrational had been placed so high that it effectively excluded any consideration by the domestic courts of the question of whether the interference with the applicants’ rights answered a pressing social need or was proportionate to the national security and public order aims pursued, principles which lay at the heart of the Court’s analysis of complaints under Article 8 of the Convention.’ (ECtHR, *Peck v. United Kingdom*, § 100)

¹⁰⁵ P. De Hert, *Artikel 8 EVRM en het Belgisch recht, o.c.*, 40-60. Compare *Peck*: ‘In determining whether the disclosure was ‘necessary in a democratic society’, the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify the disclosure were ‘relevant and sufficient’ and whether the measures were proportionate to the legitimate aims pursued’ (ECtHR, *Peck v. United Kingdom*, § 76).

¹⁰⁶ M. Delmas-Marty, *The European Convention for the Protection of Human Rights*, Dordrecht, 1992, 71 quoted by I. Cameron., *o.c.*, 26. About proportionality see also: S. Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droits de l’homme. Prendre l’idée simple au sérieux*, Bruxelles, Bruylant/Publications des FUSL, 2002, 790 p.; W. Van Gerven, ‘Principe de proportionnalité, abus de droit et droits fondamentaux’, *Journal des Tribunaux*, 1992, 305-309.

information; the use made of the data and the safeguards implemented.¹⁰⁷ A strict proportionality test, coming close to the common standard with regard to Article 10 ECHR, will be applied in the case of secret surveillance,¹⁰⁸ interceptions of letters to legal advisors,¹⁰⁹ use of (data gathered by) telephone tapping and very sensitive data that can easily be used in a discriminatory way.¹¹⁰

Our discontent partly results from observations that we have already made. First, there are comparatively few Strasbourg judgement's that offer criteria for excessive, unnecessary or and unjustified collection of processing of data. One of the factors accounting for this is the overstretched focus of the Court on the legality requirement. Of course no one can object to the Court's ruling that a legal basis in law has to exist, but also has to fulfil quality requirements such as 'foreseeability' and 'accessibility', but the assessment of these supplementary requirements often necessitates an analysis of issues that are more concerned with the rule of law guarantees foreseen in Article 6 ECHR (fair trial) and Article 13 ECHR (effective remedy). What is the added value of considering these issues under Article 8 ECHR? Secondly, based on our experience with this case law we believe that many Court judgements allow processing authorities much leeway. Only flagrant abuse or risky use of data that can easily be used in a discriminatory way is very closely scrutinised, whereas other kinds of processing of data are left untouched 'as long that there is no blood'. Attempts to challenge data protection unfriendly choices with regard to, e.g. Eurodac or passenger data, based on the 'necessity requirement, are very likely to be unsuccessful. Debates about these data protection issues do not seem to be a major concern in Strasbourg.

Only partial recognition of data protection under the scope of Article 8 ECHR

The attitudes of judges can change and the foregoing analysis is therefore far from final or decisive. Let us be cautious. The very basis of data protection recognition in Strasbourg is not as solid as it looks. Although the concept of autonomy and a large notion of personal data are brought under Article 8 ECHR, and although cases such as *Klass*, *Leander*, *Amann*, *P.G. and J.H.* and *Perry* show the Courts willingness to go beyond the traditional restricted concept of privacy defined as intimacy, it is important to see that basic data protection assumptions are not incorporated in the Strasbourg protection. Both the former Commission and the Court have held that not all aspects of the processing of personal data are protected by the ECHR. In the *Leander* case the Court stated that the refusal to give Leander access to his personal data falls within the scope of Article 8 ECHR.¹¹¹ A claim for access therefore can be based upon the same article.¹¹² But the Court also stipulated rather bluntly that this did not mean that Article 8 ECHR gives a general right to access to personal data.¹¹³ By contrast, in data protection, a general right to access is explicitly recognised, with a special arrangement for personal data kept by police and security services.¹¹⁴

Also, the Court made a distinction between personal data that fall within the scope of Art. 8 ECHR and personal data that do not. In the eyes of the Court there is processing of personal

¹⁰⁷ Compare L. Bygrave, 'Data protection law in context, particularly its interrelationship with human rights', February 2007, (4p.), p. 3 (via [://www.uio.no/studier/emner/jus/jus/JUR5630/v07/undervisningsmateriale/lecture207.doc](http://www.uio.no/studier/emner/jus/jus/JUR5630/v07/undervisningsmateriale/lecture207.doc))

¹⁰⁸ 'Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions' (ECtHR, *Klass v. Germany*, § 42)

¹⁰⁹ ECtHR, *Campbell v. United Kingdom*, Application no. 13590/88, Judgement of 25 March 1992, § 45.

¹¹⁰ 'In view of the highly intimate and sensitive nature of information concerning a person's HIV status, any State measures compelling communication or disclosure of such information without the consent of the patient call for the *most careful scrutiny* on the part of the Court, as do the safeguards designed to secure an effective protection' (ECtHR, *Z v. Finland*, § 96).

¹¹¹ ECtHR, *Leander v. Sweden*, § 48.

¹¹² ECtHR, *Antony and Margaret McMichael v. United Kingdom*, § 91.

¹¹³ ECtHR, *Gaskin v. United Kingdom*, § 37. In the case of McMichael the right to access is again recognised. Cf. ECtHR, *Antony and Margaret McMichael*, § 9. But, just as in the Leander case, a general right of access to personal data is not granted. In this case the Court does not explicitly deny such a right, but it 'simply' does not mention the issue.

¹¹⁴ See Article 8 and 9 of the 1981 Convention and Article 12 and 13 of the 1995 Directive.

data that affects private life and processing of personal data that does not affect the private life of individuals.¹¹⁵ Data protection regulation, on the contrary, does not distinguish different sorts of personal data on the basis of such thing as ‘intrinsic privacy-relevance’. The central notion of data protection is ‘personal data’, meaning any information relating to an identified or identifiable individual.¹¹⁶ Data protection, although it recognises the existence of a special category of sensitive data,¹¹⁷ is built up upon the idea that *all* personal data can be abused, including the more ordinary ones, such as names and addresses: the basic idea of data protection is to offer protection to all personal data (and a stronger protection to some types of sensitive data). This idea is without doubt based on common sense, since there can be a debate about the extent to which ordinary data should be protected, but there can be little or no debate about the idea that some protection must be granted to such data. As an example consider the following: while prohibiting the processing of sensitive data about, for instance, Jewish people, is positive, it would be unwise not to observe that a simple list of names (ordinary data) can also convey the information required to target them, and ought to be protected as well. Often, technical people favour an Internet without law and especially without data protection law considering this to be too bureaucratic or formal. It is amusing to note that those most familiar with the possibilities of ICT themselves oppose the idea that it can make sense to protect data such as names or data regarding consumer behaviour (e.g. clients of a Kosher e-market).

In cases such as *Amann*, *Rotaru* and *P.G. and J.H.*, the European Court seems to cover all these differences between its case law and the principles of data protection by applying a very broad privacy definition, an uncritical reference to the Leander case, a generous reference to the 1981 Council of Europe Convention and a very loose scrutiny of the requirements of the first paragraph of Article 8 ECHR.¹¹⁸ However, these cases should be carefully interpreted. The reference to existing data protection treaties is formulated in a way that leaves room for

¹¹⁵ A good example is the 1998-case *Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium*. Cf. ECommHR, *Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium*, Decision of 14 January 1998 on the applicability of the applications No. 32200/96 and 32201/96 (joined), Decisions and Reports, 1999, 92-98; *Algemeen Juridisch Tijdschrift*, 1997-1998, Vol. 4, 504-508. In these two joint Belgian cases the applicants complain about the absence of legislation on filming for surveillance purposes where the data obtained is not recorded in Belgium. The application was held inadmissible on the following grounds: ‘In order to delimit the scope of the protection afforded by Article 8 against interference by public authorities in other similar cases, the Commission has examined whether the use of photographic equipment which does not record the visual data thus obtained amounts to an intrusion into the individual’s privacy (for instance, when this occurs in his home), whether the visual data relates to private matters or public incidents and whether it was envisaged for a limited use or was likely to be made available to the general public. In the present case, the Commission notes that the photographic systems of which the applicant complains are likely to be used in public places or in premises lawfully occupied by the users of such systems in order to monitor those premises for security purposes. Given that nothing is recorded, it is difficult to see how the visual data obtained could be made available to the general public or used for purposes other than to keep a watch on places. The Commission also notes that the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person. Therefore, all that can be observed is essentially public behaviour. The applicants have also failed to demonstrate plausibly that private actions occurring in public could have been monitored in any way. Applying the above criteria, the Commission has reached the conclusion that there is, in the present case, no appearance of an interference with the first applicant’s private life. It follows that this part of the application is manifestly ill-founded within the meaning of Article 27, § 2 of the Convention’.

¹¹⁶ See Article 2(a) of the 1981 Convention and Article 2(a) of the 1995 Directive.

¹¹⁷ See on ‘sensitive data’, viz personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health, sexual life of data relating to criminal convictions, Article 6 of the 1981 Convention and Article 8 of the 1995 Directive.

¹¹⁸ For instance in ECtHR, *Amann v. Switzerland*, § 65-57: ‘The Court reiterates that the storing of data relating to the ‘private life’ of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgement of 26 March 1987, *Series A*, No. 116, 22, § 48). It points out in this connection that the term ‘private life’ must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of ‘private life’ should be taken to exclude activities of a professional or business nature (see the *Niemietz*, § 29 and *Halford v. United Kingdom*, judgement of 25 June 1997, § 42). That broad interpretation tallies with that of the Council of Europe’s Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985, whose purpose is ‘to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him’ (Article 1), such personal data being defined as ‘any information relating to an identified or identifiable individual’ (Article 2). In the present case the Court notes that a card on the applicant was filled in which stated that he was a ‘contact with the Russian embassy’ and did ‘business of various kinds with the company [A.]’. See paragraphs 15 and 18 above. The Court finds that those details undeniably amounted to data relating to the applicant’s ‘private life’ and that, accordingly, Article 8 is applicable to this complaint also’.

discretion.¹¹⁹ A closer reading shows that the old distinction between ‘data that merits protection’ and ‘data that does not’ is still at work and that processing of data is excluded from the privacy scope when (1) the data as such are not considered as private, (2) when there are no systematically stored images or sound recordings, or other data, (3) when the data are not systematically stored with the focus on the data subject, and (4) when the data subject could reasonably expect the processing.¹²⁰ This explains the hesitation of the Court in *P.G. and J.H.* to put police use of listening devices in a police station (par. 52 et seq.) on the same level of protection as police use of a covert listening device in a suspect's flat (par 35 et seq.). Considering the latter under the scope of Article 8 ECHR is less troublesome for the Court, whereas from a data protection perspective there is no difference when applying its principles. The same can be said of the Court's hesitation to consider ordinary camera surveillance in the streets¹²¹ and commercial metering of telecommunication data for billing purposes¹²² as falling under the scope of Article 8.1 ECHR, whereas there is no doubt about the applicability of data protection principles to these ‘legitimate’ processing applications of data.

A constructive look at the Strasbourg data protection acquis

There are many reasons to focus on the added value that Strasbourg can and does offer to data protection regulation. Without having at its disposal an explicit data protection right, the Court has brought many data protection aspects under the scope of Article 8 of the Convention. With more authority than any other possible existing institution, the Strasbourg Court has expressed the view that the protection of personal data is fundamentally important to a person's enjoyment of his or her right to respect for private life. Through its references to the 1981 Data Protection Convention, the Strasbourg Court has endorsed and spread the idea that data protection is more than just technical regulation. Hustinx rightly states that in the Court's view, Article 8 ECHR *probably* includes the obligation to give effect to the basic principles laid down in Convention 108, *in any case with respect to sensitive data*.¹²³ In doing so the Court has put some additional constitutional pressure on the implementation of this Convention.¹²⁴

We could endlessly expand on the benefits of the Strasbourg case law for data protection,¹²⁵ but in the foregoing we have also critically underlined some of the shortcomings of the Strasbourg reception of data protection: not all data are protected; the recognition of the rights to information and access is far from straightforward and, there is a shortage of information on the necessity requirement and the relevance of other Convention rights such as those

¹¹⁹ Even when these cases show a willingness to protect aspects of ‘public privacy’ and the day may come that the Court will grant Article 8 ECHR-protection to all personal data; there remain other questions to be answered, such as, just to mention one, the question whether a right to access and correction can be considered as an integral part of rights contained in Article 8 ECHR. As long as these questions are not answered, there remains undeniably a proper role to play for data protection.

¹²⁰ H.R. Kranenborg, *o.c.*, pp. 311-312.

¹²¹ ECtHR, *Perry v. the United Kingdom*, § 40: ‘As stated above, the normal use of security cameras *per se* whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention’.

¹²² ECtHR, *P.G. and J.H. v. the United Kingdom*, § 42: ‘It is not in dispute that the obtaining by the police of information relating to the numbers called on the telephone in B's flat interfered with the private lives or correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat. The Court notes, however, that metering, which does not *per se* offend against Article 8 if, for example, done by the telephone company for billing purposes, is by its very nature to be distinguished from the interception of communications which may be undesirable and illegitimate in a democratic society unless justified (see *Malone*, cited above, pp. 37-38, §§ 83-84)’.

¹²³ P.J. Hustinx, *l.c.*, p. 62 (italics added).

¹²⁴ E. Brouwer, *o.c.*, pp. 131-151

¹²⁵ In data protection all data is in principle treated alike, whether it is written, visual or other information. Rightfully the Court stresses the particular dangers of visual data as opposed to other data in ECtHR, *Von Hannover v Germany*, Judgement of 24 June 2004, § 59: ‘Although freedom of expression also extends to the publication of photos, this is an area in which the protection of the rights and reputation of others takes on particular importance. The present case does not concern the dissemination of ‘ideas’, but of images containing very personal or even intimate ‘information’ about an individual. Furthermore, photos appearing in the tabloid press are often taken in a climate of continual harassment which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution’.

contained in Article 6 and 13 ECHR, due to the Courts preference to include the idea behind the rights in its analysis of the legality requirement under Article 8 ECHR.

Still, it is better explore what more Strasbourg can do, rather than to focus upon what it does not do for the protection of those whose data are engaged. It is not unreasonable to assume that some further input can be expected from the right to equality and non-discrimination, especially since the right enshrined in Article 14 ECHR is now complemented with a more autonomous right to equality and non-discrimination contained in Article 1 of the 12th Protocol to the ECHR that came into force on the 1st of April 2005. In *Segerstedt-Wiberg and Others v. Sweden*, a claim concerning unsuccessful requests to view records held by the Swedish Security Police was refused on the grounds that making them available might threaten national security or hinder police activities. The Court not only found certain violations of Article 8 ECHR,¹²⁶ but also of Articles 10 ECHR (freedom of expression) and 11 ECHR (freedom of association). The Court considered that the storage of personal data related to political opinion, affiliations and activities that had been deemed unjustified for the purposes of Article 8, constituted an unjustified interference with the rights protected by Articles 10 and 11 concerning all the applicants, except Segerstedt-Wiberg.¹²⁷

Recently Birte Siemen has been examining the data protection rights guaranteed by the procedural rights under Articles 5, 6, and 13 ECHR. Articles 5 and 6 are only applicable in the context of a court procedure or imprisonment. In these procedures they guarantee full access rights. However, beyond these procedures, they only offer a limited added value with regard to the data subject's right of access. Siemen rightly highlights the impact of Article 6 and especially Article 13 on the right of remedy. Both supplement Article 8 ECHR in a useful way and expand significantly the legal protection of the data subject.¹²⁸ This point is well illustrated by *Segerstedt-Wiberg and Others v. Sweden*. In this case the applicants, confronted with a refusal to view records held by the Swedish Security Police, raised among others a violation of Article 13 ECHR (right to an effective remedy). The Court observed that the Swedish Parliamentary Ombudsman and Chancellor of Justice could receive individual complaints and had a duty to investigate them to ensure that the relevant laws had been properly applied. However, they lacked the power to render a legally-binding decision. Therefore, the Court found neither remedy to be effective within the meaning of Article 13 for all of the applicants. In identical terms the Court regarded as unsatisfactory the powers of the Records Board (empowered to monitor on a day-to-day basis the Secret Police's entry and storage of information and compliance with the Police Data Act). The Court noted that the Records Board had no competence to order the destruction of files or the erasure or rectification of information kept in the files. Even more significant is a similar ruling on the competences of the Swedish Data Inspection Board. This authority has wider powers than the Records Board. It has the power to examine individual complaints and to order the processor, on payment of a fine, to stop unlawful processing information other than for storage. The Board was not itself empowered to order the erasure of unlawfully stored information, but could make an application for such a measure to the County Administrative Court. However, the European Court had received no information indicating the effectiveness of the Data

¹²⁶ With regard to alleged violation of Article 8 and the storage of applicants' information, the Court held that the storage of the information had a legal basis under the 1998 Police Data Act. In addition, the scope of the discretion conferred on the competent authorities and the manner of its exercise was indicated with sufficient clarity. The Court also accepted that the storage of the information in question pursued legitimate aims, namely the prevention of disorder or crime, in the case of *Segerstedt-Wiberg*, and the protection of national security, for the other applicants. The Court concluded that the continued storage of the information that had been released was necessary concerning *Segerstedt-Wiberg*, but not for any of the remaining applicants. In terms of the refusal to grant full access to the information, the Court held that Sweden was entitled to consider national security interests and the fight against terrorism over the interests of the applicants.

¹²⁷ ECtHR, *Segerstedt-Wiberg and others v. Sweden*, § 107

¹²⁸ B. Siemen, *o.c.*, p. 204-211. See also P. De Hert, [Human Rights and Data Protection. European Case law 1995-1997], *l.c.*, p. 75-90; E. Brouwer, *o.c.*, 147 ff.

Inspection Board in practice. It had therefore not been shown that this remedy was effective.¹²⁹ In the view of the Court, those shortcomings were not consistent with the requirements of effectiveness in Article 13 and were not offset by any possibilities for the applicants to seek compensation.¹³⁰ The Court found that the applicable remedies, whether considered on their own or together, could not satisfy the requirements of Article 13 and that there had therefore been a violation of Article 13. Brouwer rightfully devotes a lot of attention to this case showing that data protection justice must not only be seen, but also be done.¹³¹ The added value of data protection authorities is assessed in practice, not in theory. When there are no positive performance indicators, then the European Court on Human Rights will not give its blessing.

II.2. Data protection tested in Luxembourg

Let us now turn to the reception of data protection by the Luxembourg Court of Justice.

Österreichischer Rundfunk and Lindqvist

Several judgements have been pronounced by the European Court of Justice (ECJ) on matters regarding the scope of application of the Directive 95/46/EC. Two of them should be mentioned here: *Österreichischer Rundfunk* and *Lindqvist*.¹³² These cases demonstrate that judicial authority also plays a full role in the process of harmonisation, since the judges of the European Court of Justice are clearly asserting the full application of the Directive.

The first decision, *Österreichischer Rundfunk*, addressed the question whether it was legally tenable to convey information regarding the income of civil servants to both the Austrian public and to the Austrian Rechnungshof (Court of Auditors) according to a national Austrian Act that pursued objectives in the public interest in the field of public accounts budget control and transparency.¹³³ Several organisations resisted the law and argued that it violated Directive 95/46/EC. The question whether Directive 95/46/EC applied to these matters was put before the ECJ by the *Rechnungshof* (Court of Audit) and by Ms Neukomm and Mr Lauer mann and their employer Österreichischer Rundfunk (ÖRF). The *Rechnungshof* and the Austrian Government held that Directive 95/46 was not applicable, since the control activity in the contested Austrian Act did not fall within the scope of Community law and showed no link with Internal Market issues. The Luxembourg Court was therefore asked to judge whether the Data Protection Directive, focusing on internal market issues, was also applicable in the case of processing undertaken by a public authority in the context of its public mission. In the second decision, *Lindqvist*, a woman working voluntarily for her local church, had published information concerning an illness suffered by another voluntary worker on the

¹²⁹ ECtHR, *Segerstedt-Wiberg and others v. Sweden*, § 120.

¹³⁰ ECtHR, *Segerstedt-Wiberg and others v. Sweden*, § 121.

¹³¹ E. Brouwer, *o.c.*, 147.

¹³² ECJ, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauer mann (C-139/01) v Österreichischer Rundfunk*, Judgement of 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01, *European Court reports*, 2003, p. I-04989; ECJ, 6 November 2003, Case C-101/01, (*Lindqvist*), *European Court reports*, 2003, p. I-12971.

¹³³ On this case: H. Kahlert, 'Einheitliches Schutzniveau für personenbezogene Daten in der Gemeinschaft', *European Law Reporter*, 2003 p.286-287; C. Haguenu-Moizard & N. Moizard, 'Informations concernant les salariés et protection des bases de données', *Revue de jurisprudence sociale*, 2003, p.945-949; J.-M. Belorgey, St. Gervasoni, & Ch. Lambert, 'Jusqu'ou peut aller la transparence dans la rémunération des dirigeants du secteur public?', *L'actualité juridique; droit administratif*, 2003, p.2149-2150; P. Miguel Asensio, 'Avances en la interpretación de la normativa comunitaria sobre protección de datos personales', *Diario La ley*, 2004 n° 5964 p.1-8; P. Blok, 'Inkomens, Internet en informatieprivacy', *Nederlands tijdschrift voor Europees recht*, 2004 p. 30-36; B. Siemen, 'Grundrechtsschutz durch Richtlinien / Die Fälle Österreichischer Rundfunk u.a. und Lindqvist', *Europarecht*, 2004 p.306-321; M. Ruffert, 'Die künftige Rolle des EuGH im europäischen Grundrechtsschutzsystem', *Europäische Grundrechte-Zeitschrift*, 2004 p. 466-471; L. Mormile, 'Trattamento dei dati personali per finalità pubbliche: il giudice del rinvio arbitro di un difficile bilanciamento', *Europa e diritto private*, 2004 p. 691-708.

parochial website.¹³⁴ Before the ECJ Ms. Lindqvist challenged the applicability of the Data Protection Directive to information published on a non-structured website.

In both cases, the Court asserted the applicability of the Directive : it ruled that the Directive was to be applied as a general rule and that its non-application should represent an exception to be considered narrowly.¹³⁵ In *Österreichischer Rundfunk* the Court recalls its former case law that internal market inspired Community Law does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis. In *Lindqvist* the ECJ found that the main principles of Directive 95/46/EC apply to using personal data on websites. The act of referring, on an Internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes ‘the processing of personal data wholly or partly by automatic means’ within the meaning of Article 3(1) of Directive 95/46. Although the EJC accepted that Ms. Lindqvist’s processing activities were not economic but had charitable and religious aims, it held that such processing of personal data was not covered by any of the exceptions listed in Article 3, paragraph 2 of the Directive, including the second exception, provided for by the second indent of paragraph 2 ‘activities which are carried out in the course of private or family life of individuals’. This exception could not be invoked when the processing of personal data consist in publication on the Internet so that those data are made accessible to an indefinite number of people (see **paras** 27, 38, 43-48).¹³⁶

Both decisions make it clear that the EU 1995 Directive has a wide scope and that it is the standard reference point within the European Information Society context, although some of its provisions, particularly those on international data transfer, ‘do not fit well to the new realities of the Internet’.¹³⁷

¹³⁴ See on the Lindqvist judgement: H. Kahlert, ‘Personenbezogene Daten im Internet’, *European Law Reporter*, 2003, p.435-437; A. Roßnagel, ‘EuGH: Personenbezogene Daten im Internet’, *Multimedia und Recht*, 2004, p.99-100; P. Miguel Asensio, ‘Avances en la interpretación de la normativa comunitaria sobre protección de datos personales’, *Diario La ley*, 2004, n° 5964 p.1-8; R. Winkelhorst & T. Van der Linden-Smith, ‘Persoonsgegevens op Internet’, *Nederlands juristenblad*, 2004, p.627-631; Kl. Taraschka, ‘Auslandsübermittlung’ personenbezogener Daten im Internet’, *Computer und Recht*, 2004, p.280-286; L. Burgogue-Larsen, ‘Publication de données à caractère personnel sur Internet, liberté d’expression et protection de la vie privée’, *Recueil Le Dalloz*, 2004, Jur., p.1062-1063; B. Siemen, ‘Grundrechtsschutz durch Richtlinien / Die Fälle Österreichischer Rundfunk u.a. und Lindqvist’, *Europarecht*, 2004, p.306-321; M. Siano, ‘La pagina Internet non ‘esporta’ dati all’estero: la Corte di giustizia definisce l’ambito di applicazione della direttiva sulla tutela dei dati personali e sulla loro libera circolazione’, *Diritto pubblico comparato ed europeo*, 2004, p.461-469; Fl. Mariatte, ‘Protection des données personnelles’, *Europe*, 2004, Janvier Comm. n° 18 p.19-21; F. Hörlsberger, ‘Veröffentlichung personenbezogener Daten im Internet’, *Österreichische Juristenzeitung*, 2004, p.741-746; R. Panetta, ‘Trasferimento all’estero di dati personali e Internet: storia breve di una difficile coabitazione’, *Europa e diritto private*, 2004, p.1002-1017; G., Cassano, ‘Cimino, Iacopo Pietro: Qui, là, in nessun luogo...Come le frontiere dell’Europa si aprirono ad Internet: cronistoria di una crisi annunciata per le regole giuridiche fondate sul principio di territorialità’, *Giurisprudenza italiana*, 2004, p.1805-1809; P. De Hert & W. Schreurs, ‘De bescherming van persoonsgegevens op het Internet: nuttige verduidelijking door de rechtspraak’, noot bij HvJ, 6 november 2003 (Bodil Lindqvist t. Zweden), *Auteur & Media*, 2004/2, p. 127-138; K. Rosier, ‘ECJ decides on protection of personal data on the Internet’, *Stibbe ICTlaw Newsletter*, 2004, No. 13, pp. 2-3

¹³⁵ In the opinion of the Court, one such exception was laid down in Article (2) in relation to both common foreign and security policy and police and judicial co-operation. The Court rejected the argument for so-called “minimal harmonisation” which, in the Court’s opinion, contradicted the “total harmonisation” goal of the Directive. The Member States should cease departing from the commonly agreed framework achieved by the Directive. See Yves Poulet, ‘EU data protection policy, The Directive 95/46/EC: Ten years after’, *Computer law & security report*, 2006, 206-217.

¹³⁶ A second question submitted to the Court was whether or not the fact of loading personal data on an Internet site, thereby making those data accessible to anyone who connects to the Internet, including people in a third (non EU) country was to be considered as a ‘transfer [of data] to a third country’ within the meaning of Directive 95/46 intended to allow the Member States to monitor transfers of personal data to third countries and to prohibit such transfer where they do not offer an adequate level of protection. The Court ruled that such processing is no transfer to third countries within the meaning of Article 25 of Directive 95/46. Another interpretation would result in an impossible situation where Member States would have to be obliged to prevent any personal data being posted on Internet sites as soon as one of the countries from where the web pages were accessible could be considered as not ensuring an adequate level of protection required by the Directive. Hence one cannot presume that Article 25 applies to the loading, by an individual in Mrs Lindqvist’s position, of data onto an Internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them (see §§ 63-64, 68, 71).

¹³⁷ P.J. Hustinx, *l.c.*, p. 62.

Österreichischer Rundfunk was the Court of Justice's first decision on Directive 95/46/EC and it is particularly interesting for our constitutional inquiry. The ECJ recalls the essential 'internal market' rationale of the 1995 EU Directive,¹³⁸ but in the same time it also strongly emphasises the human rights rationale of the Directive. Indeed it considered that the provisions of the Directive, in so far as they govern the processing of personal data liable to infringe fundamental freedoms (in particular the right to privacy), *must necessarily be interpreted in the light of fundamental rights*, which form an integral part of the general principles of law whose observance the ECJ ensures.¹³⁹ Crucial principles and references in the Directive regarding lawful processing (as for example in Article 6 and 7 of the Directive) must be ascertained on basis of criteria drawn from Article 8 ECHR, viz legality, legitimacy and necessity.¹⁴⁰

Of course this emphasis should be welcomed from a constitutional perspective, but there nevertheless remains some reason for constitutional concern. Although at the time of the Judgement, the EU Charter was known and referred to by the Advocates Generals and the Court of First Instance, the ECJ makes not a single reference to the constitutional status of data protection in Article 8 of the Charter.¹⁴¹ On the contrary, there is an almost absolute focus on the right to privacy enshrined in Article 8 ECHR as the main source of interpreting the Directive. The EC Directive 95/46 *must* be interpreted in accordance with the right to private life as protected in Article 8 ECHR.¹⁴² A breach of the right to privacy implies an unlawful processing in the sense of the Directive;¹⁴³ no breach of privacy implies no breach of the Directive. *Data protection as privacy*, no more no less.¹⁴⁴ This narrow perspective on data protection explains why the Court finds no (privacy) problem in the communication of data to third parties.¹⁴⁵

¹³⁸ ECJ, *Österreichischer Rundfunk*, §. 42: 'In those circumstances, the applicability of Directive 95/46 cannot depend on whether the specific situations at issue in the main proceedings have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty, in particular, in those cases, the freedom of movement of workers. A contrary interpretation could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations'.

¹³⁹ ECJ, *Österreichischer Rundfunk*, §. 68: 'It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case law, form an integral part of the general principles of law whose observance the Court ensures (see, inter alia, Case C-274/99 P Connolly v Commission [2001] ECR I-1611, paragraph 37)'.

¹⁴⁰ ECJ, *Österreichischer Rundfunk*, §. 66-72.

¹⁴¹ By the end of April 2003, the Advocates General had referred to the Charter in 34 cases they handled concerning human rights since the Charter's proclamation in December 2000. The Court of First Instance made its first reference to the Charter of Fundamental Rights in a case involving max. mobil, an Austrian mobile phone operator, and the European Commission (Court of First Instance, *max.mobil Telekommunikation Service GmbH v Commission* Case T-54/99, Judgement of 30 January 2001). Notwithstanding the pressure by the AG's, the EJC did not follow the example and did not refer to the Charter. See for a detailed discussion of the recognition of the Charter in the case law: http://www.jeanmonnetprogram.org/conference_lapietra/ecfr.html. A (negative) reference to the Charter is made by the United Kingdom in ECJ, 20 May 2003, (*Österreichischer Rundfunk*), §. 56: 'The United Kingdom Government submits that (...) the provisions of the Charter of Fundamental Rights of the European Union, proclaimed in Nice on 18 December 2000 (*O.J.*, No. C 364, 2000 p. 1), to which the Verfassungsgericht briefly refers, are of no relevance'.

¹⁴² ECJ, *Österreichischer Rundfunk*, §. 68

¹⁴³ See ECJ, *Österreichischer Rundfunk*, §. 91 where the ECJ rules that when national courts conclude that national legislation is incompatible with Article 8 ECHR, that legislation is also incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46, and where the ECJ also rules that that each of the exceptions included in Article 13 of that Directive must comply with the requirement of proportionality with respect to the public interest objective being pursued. In the words of the ECJ: 'that provision cannot be interpreted as conferring legitimacy on an interference with the right to respect for private life contrary to Article 8 of the Convention.'

¹⁴⁴ According to the ECJ, if national courts were to conclude that the national legislation with regard to the processing of personal data is incompatible with Article 8 of the Convention, that legislation would also be 'incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46' (ECJ, *Österreichischer Rundfunk*, §. 91).

¹⁴⁵ ECJ, *Österreichischer Rundfunk*, §. 74: 'It necessarily follows that, while the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the Convention'.

The foregoing shows that the ECJ uses a number of criteria drawn from Article 8 ECHR to evaluate the lawfulness of disputed processing.¹⁴⁶ Paragraph 83 of *Österreichischer Rundfunk* even suggests a strict proportionality test when assessing the necessity requirement.¹⁴⁷ Hence there should be no reason for concern when the European Parliament challenged the necessity of a deal concluded by the European Commission before the ECJ allowing the transfer of 34 categories of passenger data to the United States. However, the ECJ equally underlines that, according to the European Court of Human Rights (ECHR), the scope of the national authorities' margin of appreciation on the proportionality of measures can vary depending on the nature of the legitimate aim pursued and on the particular nature of the interference involved,¹⁴⁸ implying that the national authorities' margin of appreciation is especially wide in relation with measures approved for security and anti-terrorism purposes.

The PNR case

Since January 2003, European airlines flying to the United States have been obliged by the US to provide the US customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as 'Passenger Name Records' (hereinafter 'PNR data'). Based on US laws adopted following the terrorist attacks of 9/11, airline companies are obliged to submit the data before or immediately after the airplane takes off and, if they fail to do so, they can be fined a maximum of \$5,000 for each passenger whose data have not been appropriately transmitted. The PNR data comprise 34 fields of data, including not only name and address, but also contact details, such as telephone numbers, e-mail addresses, information on bank numbers and credits cards, and also on the meals ordered for the flight. The US demand for data held by European firms for billing purposes without the consent of the passengers to the transfer or a proper legal basis clearly violated several European data protection regulations. The European Commission tried to solve the problem by negotiating with the US officials a series of requirements and subsequently adopting a Decision 2004/535/EC on adequacy based on Article 25 EC Directive on Data Protection,¹⁴⁹ whose adoption meant that the Commission was convinced that the US would ensure an adequate level of data protection for the transfers. This decision enabled the Council to adopt the Agreement of 17 May 2004 between the European Community and the United States of America to officially allow the transfers. This Agreement was incorporated in Decision 2004/496.¹⁵⁰ When negotiating these instruments, the Commission, followed by the Council, assumed that it was competent to do so on the basis of the provisions in Community law regarding transportation and data protection.

Before the EJC the European Parliament raised several pleas for annulment of both the decision on adequacy and the Council 2004/496, concerning and incorrect application of the Directive, the incorrect choice of Article 95 EC as legal basis for Decision 2004/496 and breach of, respectively, the second subparagraph of Article 300(3) EC, Article 8 of the ECHR, the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith. With regard to the first two pleas (incorrect reading of the Directive

¹⁴⁶ P.J. Hustinx, *l.c.*, 63

¹⁴⁷ ECJ, *Österreichischer Rundfunk*, §. 83: 'According to the European Court of Human Rights, the adjective 'necessary' in Article 8(2) of the Convention implies that a 'pressing social need' is involved and that the measure employed is 'proportionate to the legitimate aim pursued' (see, inter alia, the Gillow v. the United Kingdom judgment of 24 November 1986, *Series A*, No. 109, § 55). The national authorities also enjoy a margin of appreciation, 'the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved' (see the Leander v. Sweden judgment of 26 March 1987, *Series A*, No. 116, § 59)'.

¹⁴⁸ ECJ, *Österreichischer Rundfunk*, §. 83 (see the foregoing footnote).

¹⁴⁹ Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under doc no C (2004) 1914), *O.J.*, No. L 235, 6 July 2004, p. 11-22.

¹⁵⁰ Council Decision 2004/496/EC on the conclusion of an agreement between the European Community and the US on the processing and transfer of PNR ('Passenger Name Records') data, *O.J.*, No. L 183, 20 May 2004, p. 83-85

and incorrect choice of Article 95 EC as legal basis for Decision 2004/496), the Parliament submitted that:

-the adoption of the Commission decision on adequacy infringed Article 3(2) of the Directive, relating to the exclusion of activities which fall outside the scope of Community law.¹⁵¹

-that Article 95 EC did not constitute an appropriate legal basis for Decision 2004/496.¹⁵² The decision did not have as its objective and subject-matter the establishment and functioning of the internal market by contributing to the removal of obstacles to the freedom to provide services and it did not contain provisions designed to achieve such an objective. Its purpose is to make lawful the processing of personal data that is required by United States legislation. Nor could Article 95 EC justify Community competence to conclude the Agreement, because the Agreement relates to data processing operations which are excluded from the scope of the Directive.

On 30 May 2006, the ECJ annulled Council Decision 2004/496/EC and Commission Decision 2004/535/EC, arguing that they could not have their legal basis in EU transport policy (a first pillar provision).¹⁵³ A careful reading of the preamble to the EU-US agreement led the EJC to find that its purposes were: to enhance security, to fight against terrorism, to prevent and combat terrorism, related crimes and other serious crimes, including organised crime; and to prevent flight from warrants or custody for those crimes.¹⁵⁴ Thus, the ECJ held that the data

¹⁵¹ Article 3.2 of the Directive is worded as follows: 'This Directive shall not apply to the processing of personal data: – in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law'.

¹⁵² The second sentence of Article 95(1) EC is worded as follows: 'The Council shall, acting in accordance with the procedure referred to in Article 251 and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.'

¹⁵³ ECJ, *European Parliament v Council of the European Union and European Parliament v Commission of the European Communities*, Joined Cases C-317/04 and C-318/04, Judgement of 30 May 2006, *O.J.*, No. C 178/2. See Sp. Simitis, 'Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz?', *Neue juristische Wochenschrift*, 2006, p.2011-2014; D. Westphal, 'Übermittlung europäischer Fluggastdaten', *Europäische Zeitschrift für Wirtschaftsrecht*, 2006, p.406-408; P. Schaar, 'EuGH-Entscheidung zur Fluggastdatenübermittlung - Grund zur Begeisterung?', *Multimedia und Recht*, 2006, p.425-426; H. Kahlert, 'Europäische Fluggastpassagierdaten in amerikanischen Händen - (kein rein kompetenzrechtliches Problem)', *European Law Reporter*, 2006, p.242-245; P. Szczekalla, 'Übermittlung von Fluggastdaten an die USA', *Deutsches Verwaltungsblatt* 2006 p.896-899; E. Pahlawan-Sentilhes, 'Coup d'arrêt aux transferts de données sur les passagers en partance pour les Etats-Unis', *Recueil Le Dalloz* 2006 IR. p.1560-1561; V. Michel, 'La dimension externe de la protection des données à caractère personnel: acquiescement, perplexité et frustration', *Revue trimestrielle de droit européen*, 2006 p. 549-559; D. Gabel & Ch. Arhold, 'Fluggastdaten (PNR): Der Beschluss des Rates über den Abschluss des Abkommens zwischen der EG und den USA über die Verarbeitung und Übermittlung personenbezogener Daten im Luftverkehr sowie die Angemessenheitsentscheidung der Kommission sind nichtig', *Europäisches Wirtschafts- & Steuerrecht – EWS*, 2006, p.363-364; E. Pedilarco, 'Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei', *Diritto pubblico comparato ed europeo*, 2006, p.1225-1231; Fl. Mariatte, 'La sécurité intérieure des États-Unis ... ne relève pas des compétences externes des Communautés', *Europe*, 2006 Juillet Etude n° 8 p.4-8; A. Mantelero, 'Note minime in margine alla pronuncia della Corte di giustizia delle Comunità europee sul trasferimento dei dati personali dei passeggeri dei vettori aerei verso gli Stati Uniti, Contratto e impresa', *Europa*, 2006, p.1075-1081; G. Tiberi, 'L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia', *Quaderni costituzionali*, 2006 p.824-829; V. Sotiropoulos, 'I 'tetarti' apofasi tou DEK schetika me tin prostasia prosopikon dedomenon - I ypohesi PNR/USA', *To Syntagma*, 2006, p.938-952; V. Sotiropoulos, 'I diavivasi prosopikon dedomenon epivatou ptiseon apo tin EE stis IPA gia skopous katapolemisis tis tromokratias - i ypohesi 'PNR/USA' sto DEK', *Efimerida Dioikitikou Dikaiou*, 2006 p.358-363; E. Dirrig, 'La jurisprudence de la Cour de justice et du Tribunal de première instance. Chronique des arrêts. Arrêt *Passenger Name Records*', *Revue du droit de l'Union européenne*, 2006, n° 3 p.698-702; M. Mendez, 'Passenger Name Record Agreement', *European Constitutional Law Review*, 2007 Vol.3 p.127-147; M. Banu, 'Protecția persoanelor fizice în privința tratamentului de date cu caracter personal. Transport aerian. Decizia 2004/496/CE. Acord între Comunitatea Europeană și Statele Unite ale Americii. Dosare ale pasagerilor aerieni transferate către Biroul vamal și de protecție a frontierelor al SUA. Directiva 95/46/CE. Articolul 25. State terțe. Decizia 2004/553/CE. Nivel adecvat de protecție', *Revista română de drept comunitar*, 2007 n° 2 p.131-134; P. De Hert & G.-J. Zwenne, 'Over passagiersgegevens en preventieve misdaadbestrijding binnen de Europese Unie', *Nederlands juristenblad*, 2007, p.1662-1670; G.-J. Zwenne & P. De Hert, 'Sur les données des dossiers passagers, la directive 'vie privée' 95/46/CE et la non-adéquation de la législation européenne', *Revue européenne de droit de la consommation*, 2007, p.223-242; P. De Hert & G.G. Fuster, 'Written evidence on the PNR Agreement', Evidence submitted to House of Lords Sub-Committee F, E/06-07/F49 PNR, 5p. submitted February 2007 via http://www.parliament.uk/parliamentary_committees/lords_s_comm_f/eufwrevid.cfm.

¹⁵⁴ ECJ, *European Parliament v Council of the European Union and European Parliament v Commission of the European Communities*, § 56-59: 'It follows that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law. While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature. As pointed out in paragraph 55 of the present judgment, that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes. The Court held in paragraph 43 of Lindqvist, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Article 3(2) of the Directive are,

transfers concerned fell within a framework established by the public authorities related to public security.¹⁵⁵ Hence, not the Commission within the first pillar, but the Council within the third pillar should have acted and negotiated with the United States.

In his initial reaction to the PNR judgment, the European Data Protection Supervisor¹⁵⁶ declared that the ruling of the ECJ had created a loophole in the protection for citizens, since it suggested that the transmission of information to third countries or organisations from European databases such as the Visa Information System or the Schengen Information System would escape the applicable rules of the 1995 Data Protection Directive, as long as the transmission is intended for police or public security use. The Court judgment has been seen as a failure for the European Parliament, as it had launched the procedures, but mainly on different grounds, namely, that Commission Decision 2004/535/EC and Council Decision 2004/496/EC accepted a disproportionate transfer of data to the United States without proper data protection guarantees. The Parliament held that the agreement and its accompanying 'adequacy' decision violated the principle of proportionality, particularly in reference to the quantity of data collected and the retention period foreseen.

The ECJ did not have the opportunity to address the argument in its judgement for the PNR case, as it annulled both the Council Decision 2004/496/EC on the conclusion of the agreement, on the one hand, and the Commission Decision 2004/535/EC holding that the US Bureau of Customs and Border Protection (CBP) offered a sufficient level of protection for personal data transferred from the EU, on the other hand, on formal grounds related to their legal basis (see above). On the contrary, Advocate General Léger's did examine the proportionality argument in his Opinion in Cases C-317/04 and C-318/04¹⁵⁷ and he did it in an extremely interesting, albeit potentially dangerous, manner, which deserves special attention. Indeed, before expressing his views of the validity of the proportionality argument, Advocate Léger's manifested a series of highly interesting remarks on the scope of the control to be exercised by the ECJ concerning proportionality. He first made reference to the ECtHR case law to declare that according to such case law interferences with private life might require a strict judicial control (§ 229). Second, he underlined that, also according to ECtHR case law, when the interferences are established with the purpose of national security or to fight against terrorism, public authorities enjoy wider discretionary powers (§ 230). Finally,

in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals. However, this does not mean that, because the PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security. It follows from the foregoing considerations that the decision on adequacy concerns processing of personal data as referred to in the first indent of Article 3(2) of the Directive. That decision therefore does not fall within the scope of the Directive'.

¹⁵⁵ L Creyf and P Van de Velde, 'PNR (Passenger Name Records): EU and US reach interim agreement', *Bird & Bird Privacy & Data Protection Update*, October 2006, No. 11, 2p. (<http://www.twobirds.com/english/publications/newsletters/>). On 3 July 2006, the Council and the Commission notified termination of the agreement with effect from 30 September 2006. On 7 September 2006, the European Parliament adopted a report in which it asked the Council to negotiate – under the Parliament's oversight – an interim agreement, whereby the Parliament wanted to ensure that the US offers adequate protection of the passenger data collected and which should provide for a change to the 'push' system (under which US authorities must request specific data which will then be selected and transferred) instead of the present 'pull' system (whereby access is granted to the full database and airline passengers data are directly accessed online by the authorities concerned). In its report, the Parliament further requested joint decision-making rights over the negotiation of the final agreement with the US. On 6 October 2006, shortly after the Court-set deadline of 30 September, EU negotiators reached an interim agreement with their US counterparts. The conflict of laws situation that has existed since 1 October 2006 thereby appears to be, at least temporarily, solved. The interim agreement would ensure a similar level of protection of the PNR data as before and it would also comply with the US request that the PNR data can be more easily distributed between different US agencies. A move from the 'pull' system to the 'push' system should be undertaken at a later date. The nature of PNR data available to US agencies remains unchanged. The interim agreement will apply from its date of signature, which is due to be completed by 18 October, and will expire no later than 31 July 2007. By this date a new (superseding) agreement should be reached between the parties who meet again in November 2006 to begin discussions on that point.

¹⁵⁶ Regulation 45/2001 of 18 December 2000 provides for supervision by a special supranational authority: the European Data Protection Supervisor, or EDPS. In 2002, the Council adopted a decision on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties (Decision no. 1247/2002 of 1 July 2002, *O.J.*, No. L 183, 12 July 2002.). The creation of the EDPS is based on Decision 1247/2002 of 1 July 2002 on the regulations and general conditions governing the performance of this organisation's duties (*O.J.*, No. L 183, 12 July 2002.).

¹⁵⁷ Léger, Philippe (2005), *Conclusions de l'Avocat Général M. Philippe Léger présentées le 22 novembre 2005*, [Opinion of the Advocate General in Cases C-317/04 and C-318/04] Luxembourg.

he concluded that, in the PNR case, the latter notion shall predominate and, therefore, judicial control could not be strict: recognising to public authorities wide discretionary powers to determine which measures are to be considered proportionate, the judicial control should limit itself to the appreciation of any possible manifest error in such assessment (§ 231). This limitation of the scope of the judicial control marked the Advocate General's analysis of the proportionality of the measures foreseen in the first PNR agreement, which he concluded to be proportionate taking into account the wide discretionary powers that, in his view, should be recognised to the EC and the Council (§ 246).¹⁵⁸

Advocate General Léger's opinion can be perceived as a worrying sign, supporting the view that citizens cannot rely on the judiciary to protect them against any intrusive security measures that public authorities might declare proportionate. Elsewhere we have highlighted that this alarming progressive self-effacement of the judiciary in its role to assess the proportionality of intrusive measures is not yet widely recognised, and therefore certain public authorities might still choose to indulge in increasingly intrusive measures in the belief that, if citizens were to judge them disproportionate, they could always refer to the courts — a conclusion which seems no longer valid.¹⁵⁹ Rather than a limited formal compliance check from our judges, we expect a strict review of all the different alternatives encountered and their different impact on privacy, and individual rights. Does the US need 34 categories of data? Why are the EU PNR agreements concluded with Australia and Canada less infringing on human rights? Are Australian and Canadian security forces wrongly less demanding or do they combine security and privacy better?¹⁶⁰

Advocate Léger's Opinion is also dramatically unsatisfactory from a data protection perspective. Here we see a case that is wholly data protection relevant. Next to the proportionality issue of the measure ('is sending passenger data to the US necessary'?), the case is loaded with pure data protection aspects. Why does the US government need these data for such a long period? Are the European passengers informed about the transfer? Is there effective supervision in the US for complaints from Europe? Who has access to the data in the US? Will it be used for specific goals? All these issues are disregarded by Léger and replaced by a very formal and simple general proportionality check that we know from the privacy case law. The old Constitution (with its leeway for governments in the area of security) is apparently still very active, and there are few indications that an independent status for data protection is a separate constitutional concern.

Future testing in Luxembourg: Public access and data protection

The right of access to documents and the right of individuals with regard to protection of their personal data are both rooted in the EC Treaty (Articles 255 and 286 respectively). They have been implemented through two Regulations: (EC) No 45/2001 on data protection (see *above*), and (EC) No 1049/2001 on public access to documents,¹⁶¹ and have been codified in the Charter of Fundamental Rights.¹⁶² The two rights can be contrastive when access is

¹⁵⁸ « *L'ensemble de ces garanties nous conduisent à considérer que, eu égard à la grande marge d'appréciation qui doit, selon nous, être reconnue en l'espèce au Conseil et à la Commission, l'ingérence dans la vie privée des passagers aériens est proportionnée au but légitime poursuivi par le régime PNR* » (underlined by the authors) (Léger, 2005:1-64).

¹⁵⁹ G.G. Fuster & P. De Hert, 'PNR and compensation: how to bring back the proportionality criterion', *BNA's World Data Protection Report*, 2007, Vol. 7, August, No. 8, pp. 4-10.

¹⁶⁰ Sophia in 't Veld and others, Joint motion for a resolution on the PNR agreement with the United States, European Parliament, 10 July 2007 (via http://www.quintessenz.org/doqs/000100003894/2007_07_11_EU-parl_PNR_joint%20resolution.pdf)

¹⁶¹ Regulation No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *O.J.*, No. L 145, 31 May 2001, pp. 43-48]

¹⁶² See Article 42 of the Charter (Right of access to documents): 'Any citizen of the Union and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents'. See also Article 41 (Right to good administration): '1. Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union. 2. This right includes:

- the right of every person to be heard, before any individual measure which would affect him or her adversely is taken;
- the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy; (...)

specifically requested to information relating to an individual. The European Data Protection Supervisor has addressed this issue in a background paper, providing useful practical guidance for handling such requests.¹⁶³

In *The Bavarian Lager Company Ltd. v Commission* (Case T-194/04) a judgement was delivered by the Court of First Instance on 8 November 2007.¹⁶⁴ The case concerned the disclosure of the names of certain people in their official public capacity (no private data was requested), the names were contained in the minutes of the meeting (no images or sound recording and no systematic and data subject focussed storage occurred) and the participants could reasonably expect disclosure since they were acting in their public capacity and participating in a meeting of the European Commission.¹⁶⁵ The Court held that access to documents containing personal data falls under Regulation No 1049/2001 and not under Regulation No 45/2001. The Court recalled that Recital 15 of Regulation No 45/2001 states that access to documents, including conditions for access to documents containing personal data, is governed by the rules adopted on the basis of Article 255 EC, concerning the right of access to documents. Article 4(1)(b) of Regulation No 1049/2001 on the public access to documents indicates that EU institutions shall refuse access to a document where disclosure would undermine the protection of 'privacy and integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data'. Community legislation includes, inter alia, Regulation No 45/2001, which establishes the conditions for certain lawful processing of personal data not requiring the consent of the data subject. Processing under the scope of Regulation No 1049/2001 is an example of such lawful processing. Considering this and the need to construe and apply restrictively exceptions to rights, the Court concluded that for the exception of Article 4(1)(b) to apply the disclosure of data should undermine the privacy and the integrity of the individual in the sense of Article 8 ECHR, in accordance with Art. 6(2) EU, and that it was not the case. Additionally, the Court stated that the Commission erred in law by holding that the applicant had to establish an express and legitimate purpose or need to obtain the disclosure of the names to which it had been refused access. Finally, the Court established that the exception to access based on arguments related to the protection of the purpose of inspections, investigations and audits [Article 4(2) of Regulation No 1049/2001] did not apply.

Of course our attention is drawn to the way the Court conceives the relation between privacy and data protection. In the judgement, the Court emphasized that the concept of 'private life' is broad and may include the protection of personal data, but not all personal data necessarily fall within the concept of 'private life', and, a fortiori, not all personal data should be considered by their nature capable of undermining the private life of the individual.¹⁶⁶ Regulation No 1049/2001 contains an exception to public access related to the privacy and the integrity of the individual, in which, according to the Court's interpretation, the main interest

¹⁶³ Public Access to Documents and Data Protection', Background Paper Series, July 2005, No 1.

¹⁶⁴ ECtF Instance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, Cases C-194/04, Judgement of 8 November 2007, *European Court reports*, 2007 (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004A0194:EN:NOT>).

¹⁶⁵ On 11 October 1996, a meeting took place attended by representatives of the Commission's Directorate-General for the Internal Market and Financial Services, the United Kingdom Department of Trade and Industry and representatives of the Confederation des Brasseurs du Marche Commun. Bavarian Lager had asked to participate at that meeting, but the Commission had refused. Following a number of requests by Bavarian Lager based on Community legislation concerning public access to documents, the Commission disclosed to it, *inter alia*, the minutes of the meeting of 11 October 1996, stating that the names of five persons who had attended that meeting had been blanked out, two of them having expressly objected to disclosure of their identity and the Commission having been unable to contact the three others. Bavarian Lager made a confirmatory request for the full minutes, containing the names of all the participants, which the Commission rejected by a decision of 18 March 2004. The Commission took the view that Bavarian Lager had not established either an express and legitimate purpose or any need for such disclosure, as was required (so it argued) by the regulation on the protection of personal data,² and that, therefore, the exception concerning the protection of private life, laid down by the regulation on public access to documents, applied. It further took the view that disclosure would compromise its ability to carry out investigations. Bavarian Lager applied to the Court of First Instance for the annulment of that decision.

¹⁶⁶ ECtFInstance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, §§ 114-115.

protected is ‘private life’, not ‘personal data’: access to documents shall be refused on the basis of such exception where disclosure would undermine the protection of privacy and integrity of the individual. The Court recalled that professional activities are not, in principle, excluded from the concept of ‘private life’ within the meaning of Article 8 of the ECHR, but they are not always included in it either. In this case the right to privacy does not apply. The mere presence of the name of a person in a list of participants at a meeting, acting on behalf of the body they represent, does not compromise the protection of the privacy and integrity of the person.¹⁶⁷

The strategy consisting in using the differences between privacy and data protection as part of the solution to solve the collision between the right to access and the right to data protection, has been proposed in literature before.¹⁶⁸ However, the ease with which the Court of First Instance uses the old constitution distinguishing two kinds of personal data does not sit comfortably with the formal constitutional codification of data protection within EU law. In vain the Commission argued that both data protection and access are rights are of the same nature, importance and degree, and have to be applied together. Where a request is made for access to a public document containing personal data, a balance must be sought on a case-by-case basis.¹⁶⁹ The reasoning of the Court is simple: since there is no privacy, data protection does not apply. However, according to Article 4 of Regulation No 1049/2001, concerning exceptions to the right of access: ‘1. The institutions shall refuse access to a document where disclosure would undermine the protection of: (...) (b) privacy and the integrity of the individual, *in particular in accordance with Community legislation regarding the protection of personal data*’ (italics added). Hence, the obligation for the Court to take data protection seriously and to apply legislation as much as possible when balancing it with other constitutional values. More specific this implies a duty for the Commission and *Bavarian Lager Company* to respect data protection principles such as non-disclosure and purpose specification. There is a whole world of options between the right not to grant access because of data protection and, the right not to grant data protection because of access. The Court should have thus taken this into consideration to achieve a better balance between the two rights.

III. CONCLUSIONS

The right to privacy is without doubt part of primary EC legislation because of its adoption in Article 8 ECHR. Although codified in the EU Charter, it is not as easy to establish whether the right to data protection as such (in a broader scope) has the same status.¹⁷⁰ The incorporation of data protection in Constitutions is probably a good political statement, but it is far too early to evaluate its legal effects. Our analysis of the case law in Luxembourg and Strasbourg reveals that the right to data protection has not yet achieved its full status.

¹⁶⁷ ECtFInstance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, §§ 121-126.

¹⁶⁸ H.R. Kranenborg, *Access to documents and data protection in the European Union. On the public nature of personal data*, Deventer, Kluwer, 2007, 351p.; P. De Hert, ‘Les données à caractère personnel et la publicité des documents administratifs’, Titre XI in P. De Hert (ed.), *Manuel sur la vie privée et la protection des données*, Bruxelles, Ed. Politéia, feuillets mobiles, mise à jour No. 6 (2001), 94p. ; DE HERT, P., ‘De grondrechten en wetten m.b.t. openbaarheid van bestuursdocumenten en bescherming van de persoonlijke levenssfeer. Analyse van de onderlinge relatie en commentaar bij het arrest Dewinter van de Raad van State’ [Comparing fundamental rights and bills with regard to privacy and freedom of information], *Publiekrechtelijke Kronieken-Chronique de Droit Public (C.D.P.K.)*, 2001, No. 4, pp. 374-425.

¹⁶⁹ ECtFInstance, *The Bavarian Lager Co. Ltd v Commission of the European Communities*, § 77.

¹⁷⁰ H.R. Kranenborg, *o.c.*, p. 313.

Previously, we quoted Lessig's observation of the need for transformative constitutions to fight harder than just codifying constitutions.¹⁷¹ This analysis is followed by some compelling paragraphs on the vulnerable role of the courts in making the Constitution materialise. For Courts to impose transformative values after the approval of a constitution is a very critical step, since they operate within a political context and are the weakest branch of resistance within that political context. Lessig notes that even a strong statement of principle enacted within a Constitution's text, allows a court only so much freedom to resist. Although the same can be said about codifying constitutions, the problem increases with regard to transformative parts of the Constitution regarding Cyberworld. When judges have to make judgments that do not seem to flow plainly or obviously from a legal text, their judgment will appear to have been politically influenced. Whenever it seems as though a Court is doing no more than simply confirming founding commitments, it creates the idea that this Court is simply acting to ratify its own views of a proper constitutional regime rather than enforcing judgments that have been constitutionalised by others. In other words, it appears to be making 'political moves.'

Our analysis needs to be enriched with an analysis of further developments, a broader analysis of human rights case law and an analysis of data protection case law in the Member States. With regard to Strasbourg case law, we need to consider judgements such as *Schenk*¹⁷² and *Khan*¹⁷³ in which the Court refuses to recognise the exclusionary rule. As regards case law, in Member States a discussion is needed regarding the English *Durant case*¹⁷⁴ and the Belgian *Court of Cassation* judgment of 27 February 2001¹⁷⁵, both demonstrating a clear willingness

¹⁷¹ L. Lessig, *o.c.*, p. 214.

¹⁷² In *Schenk* a person is charged who was criminally convicted in his own country, partly on the grounds of the recording of a telephone call made by him (ECtHR, *Schenk v. Switzerland*, Judgement of 12 July 1988, *NJCM*, 1988, 570-575; *N.J.*, 1988, N° 851. The recording was made, in secret, by the person he was phoning and was offered to the government. Schenk pleaded on the grounds of the illegality of the evidence used. The Swiss Supreme Court did not preclude that the recording fell under the applicable Swiss criminal regulations on the interception of telecommunication, but was of the opinion, after considering the interests at stake, that the recording could be used as evidence material. Schenk went to Strasbourg and stated before the Commission that the evidence material used gave his trial an unfair character in the sense of article 6 subsection 1 and 2 of the ECHR. In its report of 14 May 1987, the Commission was of the opinion that article 6 subsection 1 had not been violated. Schenk's reference to article 6 subsection 2 of the ECHR was rejected as an erroneous interpretation of this regulation. Before the Court a representative of the Commission additionally asserted that the person concerned actually was considered innocent by the Swiss judges until his guilt had been proven in accordance with the law, the view on the judgement of the Swiss courts was that the trial as a whole was 'perfectly' lawful, in spite of non-observance of a criminal regulation (*Schenk*, § 50). This rather peculiar additional argument ('no treaty violation because the Swiss judges state that everything is all right') shows that for Strasbourg the admissibility of evidence is in principle a matter for national law. This opinion is confirmed, in so many words, by the Court with the analysis of article 6, subsection 1 of the ECHR. 'While Article 6 of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law. The Court therefore cannot exclude as a matter of principle and in the abstract that unlawfully obtained evidence of the present kind may be admissible. It was only to ascertain whether Mr. Schenk's trial as a whole was fair' (*Schenk*, § 46). See in the same sense: ECtHR, *Lüdi v. Switzerland*, Judgement of 15 June 1992, § 43; ECtHR, *Vidal v. Belgium*, Judgement of 22 April 1992, § 33; ECtHR, *Dombo Beheer v. The Netherlands*, Judgement of 27 October 1993, 274, § 31; ECtHR, *Schuler-Zraggen v. Switzerland*, Judgement of 24 June 1993, § 66. In *Schenk*'s case article 6, subsection 2, ECHR has not been violated. There is no evidence in the trial records that show that he was considered guilty by the Swiss judges during the trial. Any prejudice, on the part of the judges, cannot not be derived from the addition of the recording to the evidence (*Schenk*, § 51). With regard to article 6 subsection 1 of the ECHR the Court judged earlier in the trial that this regulation was not violated: on the whole the prosecutor had a fair trial, because during the trial the person had the opportunity to dispute the facts and because the recorded material was not the only piece of evidence (ECtHR, *Schenk*, resp. § 47 and 48).

¹⁷³ ECtHR, *Khan v. United Kingdom*, judgement of 12 May 2000. The *Khan* judgement accepted that the admission of evidence obtained in breach of the privacy right against an accused person is not necessarily a breach of the required fairness under Article 6 (the right to a fair trial). Evidence was secured by the police in a manner incompatible with the requirements of Article 8 of the Convention, and yet, it was admitted in evidence against the accused and let to his conviction, since the process taken as a whole was faire in the sense of Article 6 ECHR. Compare 'applicants had ample opportunity to challenge both the authenticity and the use of the recordings'; (ECtHR *P.G. and J.H. v. the United Kingdom*, judgement 25 September 2001, § 79).

¹⁷⁴ Court of Appeal (civil division) 8 December 2003, *Michael John Durant t. Financial Services Authority*, [2003] EWCA Civ 1746. See Edwards, Lilián, 'Taking the 'Personal' Out of Personal Data: Duran v. FSA and its Impact on Legal Regulation of CCTV', *SCRIPT-ed*, Vol. 1, Issue 2, June 2004, pp. 341-349.

¹⁷⁵ Cass. 27 February 2001, *Computer*. 2001, p. 202, annotated by J. DUMORTIER., *Vigiles*, 2001, vol. 6, no. 4, pp. 153-157, annotated by P. De Hert; *R.W.*, 2001-2002, annotated by P. Humblet. The judgement that was disputed before the Court of Cassation was delivered by the Court of Appeal from Ghent, 2 February 1999, published in *RPO-T*, 2001, vol. 1, no. 2, pp. 30-33, annotated by P. De Hert. See also: P. De Hert, 'Caméras cachées dans des magasins, la controverse suite à un arrêt de cassation', *Sécurité privée*, 2001, no. 11, 27-30; P. De Hert & S. Gutwirth, 'Cassatie en geheime camera's: meer gaten dan kaas' [The *Cour de cassation* and secret camera's: more holes than cheese], *Panopticon*, 2001, pp. 309-318; P. De Hert, 'De waarde van de wet van 8 december 1992 bij de bewijsbeoordeling in strafzaken', *Tijdschrift voor Strafrecht*, 2002, Vol. 3/6, pp. 310-317.

of the local judges to reject data protection regulation implications by applying a very narrow interpretation of *personal data*. Some years ago, Bygrave observed that the role of judiciary and quasi-judicial bodies was relatively marginal.¹⁷⁶ Today there is case law but it is questionable whether the new constitutional framework provides enough personal data protection. Both Brouwer and Bygrave have warned against reducing data protection to privacy to prevent data protection issues from being too easily brushed aside as either minor or relatively insignificant matters.¹⁷⁷ So far Strasbourg and Luxembourg have only produced a few cases on the relationship between data protection and privacy, but the result is far from promising for data protection principles. Rulings such as in *Bavarian*, hesitations such as in *P.G. and J.H.* and reasoning such as in Advocate General Léger's Opinion cast doubt on the constitutional status of data protection and create the risk that data protection principles will continue to be considered 'soft law' instead of becoming 'hard law' based on a constitution.¹⁷⁸

Data protection principles might seem less substantive and more procedural compared to other rights norms, but they are in reality closely tied to substantial values and protect a broad scale of fundamental values other than privacy.¹⁷⁹ Because of its reputation of only focusing on the benefits for individuals, putting data protection in the privacy frame hampers the realisation of the societal benefits of data protection rights and therefore puts these rights essentially in conflict with the needs of 'society'.¹⁸⁰

¹⁷⁶ L. Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law', in P. Wahlgren (ed.), *IT och juristutbildning. Nordisk årsbok i rättsinformatik 2000*, Stockholm, Jure AB, 2001, pp. 113–125)

¹⁷⁷ E. Brouwer, *o.c.*, p. 206; L. Bygrave, 'The Place of Privacy in Data Protection Law', § 20.

¹⁷⁸ Compare E. Brouwer, *o.c.*, p. 206.

¹⁷⁹ E. Brouwer, *o.c.*, p. 206.

¹⁸⁰ L. Bygrave, 'The Place of Privacy in Data Protection Law', § 20.