REFGOV

Reflexive Governance in the Public Interest

Fundamental Rights

Data Protection in the EU: Towards 'Reflexive Governance'?

Gloria González Fuster and Serge Gutwirth

Working paper series : REFGOV-FR-19

Data Protection in the EU: Towards 'Reflexive Governance'?

A REFGOV Thematic Research

Gloria González Fuster and Serge Gutwirth[1]

Institute for European Studies (IES) and Law, Science, Technology & Society Studies (LSTS) Center of the Vrije Universiteit Brussel (VUB)

Last update: July 2008.

[1] The authors are indebted to Prof. Dr. Paul de Hert [LSTS (VUB) and Tilburg Institute for Law, Technology, and Society (TILT)] for his support during the completion of the research.

Index

1. Introduction

The present report is the result of the research conducted for the Fundamental Rights Sub-Network of the 'Reflexive Governance in the Public Interest' (REFGOV) project[2], a 6th Framework Programme funded by the European Commission (EC). The research explored European Union (EU) law and policy-making regarding the fundamental right to the protection of personal data. The final aim of the report is to provide suggestions for a better development of EU-level law and policy-making concerning the right to the protection of personal data. The study should also allow for the preparation of recommendations on EU law and policy-making regarding fundamental rights in general.

The first part of the report is predominantly descriptive. Section 2 offers a condensed overview of the historical evolution of the right to the protection of personal data in the EU; Section 3 reviews the main actors involved in the field, and Section 4 examines relevant current practices. The second part of the study introduces the EU governance debate, and explores the potential of the 'reflexive governance' approach to deepen our understanding of the issues at stake (section 5). Section 6 proposes recommendations based on the research's results.

The research firstly revolved around the analysis of relevant literature and legal and policy-documents. At a second stage, an expert workshop allowed for the discussion, assessment and improvement of the initial findings. The authors are extremely grateful to the workshop's participants for their very valuable feedback and suggestions.[3]

2. Data Protection In The EU: A Contrasted Evolution

The present section firstly offers a chronological table highlighting the main steps of the evolution of the right to the protection of personal data in the EU. Secondly, it summarizes the key elements of the progressive implementation of the right at EU level and, finally, it examines the major limitations and obstacles rendering problematic such implementation.

2.1. A Concise Chronology of Data Protection in the EU

To illustrate the main critical steps of the evolution of the right to the protection of personal data in the EU, the following table has been divided in three columns. Under the first column are noted the developments related to EU's 'first pillar', also known as 'Community pillar', corresponding to the three Communities: the European Community, the European Atomic Energy Community (Euratom) and the European Coal and Steel Community (ECSC). The 'third pillar' column concerns the EU pillar devoted

[2] The REFGOV Integrated Project (IP) is a five years project counting 29 partner-institutions and coordinated by the Centre for Philosophy of Law - Centre de Philosophie du Droit (CPDR) of the Catholic University of Louvain (Louvain-La-Neuve). More information on the project: http://refgov.cpdr.ucl.ac.be/.

[3] The workshop was organised at the Institute for European Studies (IES) of the Vrije Universiteit Brussel (VUB) on 16 May 2008. It took the form of the morning session of the one-day workshop "*Data Protection and Criminal Law in the European Union (EU): Towards 'Reflexive Governance'*?", in which the afternoon session dealt with EU criminal law. Participating discussants were: Rocco Bellanova (researcher), Sergio Carrera (CEPS), Willem Debeuckelaere (Privacy Commissie), Paul de Hert (IES/LSTS), Bart De Schutter (IES), Maartje De Schutter (Liga Voor Mensenrechten), Olivier De Schutter (UCL), Kees Groenendijk (Commissie Meijers), Hielke Hijmans (EDPS), Erik Josefsson (FFII), François Kristen (Universiteit Utrecht), Yves Moiny (EC,), Eugenio Mantovani (LSTS/VUB), Violeta Moreno Lax (UCL), Pieter Paepe (IES), Yves Poullet (FUNDP), Piet Hein van Kempen (Radboud Universiteit Nijmegen), Niovi Ringou (EC), Roger Smith (JUSTICE) and Martin Wasmeier (EC).

to police and judicial cooperation in criminal matters, which comes under Title VI of the EU Treaty. Under the tag 'Other', in the third column, are mentioned relevant events taking place outside the EU institutional framework.

Year	FIRST PILLAR	THIRD PILLAR	OTHER
…			
1950			**European Convention for the Protection on Human Rights (ECHR)**[4] Art. 8: right to privacy
…			
1970			Council of Europe starts discussing limitations of Art. 8 ECHR in the light of technological developments
…			
1973	Internal EC document proposes public hearings to discuss common measures to protect the citizen in the light of the creation of data banks[5]		Council Of Europe Resolution 73(22) on Privacy in the Private Sector[6]
1974			Council Of Europe Resolution 74(29) on Privacy in the Public Sector[7]
1975	Call by EP for harmonization of data protection in the EU		
…			
1979	New call by EP for harmonization of data protection in the EU		
…			
1981			**Council of Europe 'Convention No. 108' on the protection of personal data**[8]
	EC rejects calls for harmonization, suggests national implementation of 'Convention No. 108' instead		
1982	New call by EP for harmonization of data protection in the EU		
…			
1985			Germany, France and Benelux adopt Schengen Agreement
…			
1987			**Recommendation No. R(87)15 concerning the use of personal data in the police sector**[9]
			Discussions on

[4] Council of Europe (1950), The European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4 November.
[5] EC (1973), Community Policy on Data Processing: Communication of the Commission to the Council, SEC (73) 4300 final, 21 November. Referring to the need to protect the citizen, see point 39.
[6] Council Of Europe (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector.
[7] Council Of Europe (1974), Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector.
[8] Not self-executing Council of Europe's 1981 Convention on Data Protection, also known as 'Convention 108' [Council of Europe (1981), Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series, No. 108 of 28 January 1981].
[9] Council Of Europe (1987), *Recommendation No. R(87)15 concerning the use of personal data in the police sector*, adopted by the Committee of Ministers on 17 September 1987.

			computerised information system for Schengen
…			
1990			**Convention implementing the Schengen Agreement**[10]
	EC presents first draft of future 'Data Protection Directive'[11]		
…			
1992	EC presents second draft of future 'Data Protection Directive'		
…			
1994	Bangemann's Report[12]		
1995	**Customs Information System (CIS)**[13]		
		Europol Convention[14]	
	Directive 95/46/EC[15] ('Data Protection Directive') Art. 29 Working Party established		
…			
1997	Amsterdam Treaty introduces: **Art. 286 on the protection of personal data in EC institutions**[16]		
	Directive 97/66/EC[17]		
1998		'Vienna action plan'[18] mentions harmonisation of third pillar data protection	
		Call for *ad-hoc* working group on third pillar data protection launched in COREPER[19]	

[10] On 19 June 1990. The Schengen *acquis* - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, Official Journal L 239, 22.9.2000, pp. 19–62.

[11] Adopted by the EC on 18 July 1990; published in September of the same year.

[12] The approval of the Data Protection Directive was given a key impetus by a report concluded by a high-level group on European Information Infrastructures, under the chairmanship of Martin Bangemann, *Europe's way forward to the information society*, submitted to the European Council at Corfu in June 1994 [PEARCE, Graham, and Nicholas PLATTEN (1998), "Achieving Personal Data Protection in the European Union", *Journal of Common Market Studies*, Volume 36, No. 4, Blackwell Publishers, December, p. 536].

[13] Council Act 95/C316/02 of 26 July 1996 drawing up the Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes, Official Journal, C 316 of 27 November 1995, pp. 33-42 (hereafter the 'CIS Convention').

[14] Council Act of 26 July 1995 drawing up the Convention based on Article K.3d of the Treaty on European Union on the establishment of a European Police Office (Europol Convention), Official Journal, C 316 of 27.11.1995.

[15] Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal, L 281, 23.11.1995, pp. 31-50.

[16] Providing that Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data should also apply to Community institutions and bodies, and that an independent supervisory authority should be established.

[17] 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, Official Journal, L 24, 30.1.1998, pp. 1–8.

[18] Adopted by the Justice and Home Affairs Council.

[19] On 6 May 1998, the Italian delegation at COREPER asked for the creation of a working group responsible of the examination of third pillar data protection mechanisms, the possibility of establishing a series of standard

		Launching of the Group on Information Systems and Data Protection at the Council[20]	
1999	Treaty of Amsterdam transfers Asylum Policy from third to first pillar		
	Directive 99/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity[21]		
2000			**Safe Harbour agreement**[22]
		Third step work-programme for third pillar data protection adopted[23]	
	EU Charter of Fundamental Rights[24] Art. 7: right to privacy. Art. 8: right to the protection of personal data		
		Common secretariat for third pillar Joint Supervisory Authorities[25]	
2001		Application of future Regulation (EC) 45/2001 to third pillar discussed but rejected by Council[26]	
	Regulation (EC) 45/2001[27] EDPS created		
	First stage of consultation on data protection in employment		
		Draft resolution on the rules governing the protection of personal data (not adopted)	
2002	**Directive 2002/58/EC**[28]		

data protection rules and the possibility of reducing the number of authorities [BRULIN, Hughes (2003), "La protection des données: quête et errements dans le Troisième Pilier", *Actualités de Droit Pénal Européen*, Bruxelles: La Charte, p. 137].

[20] Launched on 28-29 May 1998 by the British presidency (*idem*).

[21] Directive 99/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal, L 91, 7.4.1999, pp. 10-28.

[22] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour principles and related frequently asked questions issued by the US Department of Commerce (2006/520/EC), Official Journal of the European Communities, L 215, 25.8.2000, pp. 7-47.

[23] Established by the 1999 Finnish and 2000 Portuguese presidencies, based on three axes: 1) creation of a shared secretariat for the supervisory authorities; 2) creation of a joint supervisory authority for the third pillar; 3) establishment of common principles for third pillar data protection [BRULIN, *op. cit.*, p. 137].

[24] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, C 364, 18.12.2000, pp. 1-22.

[25] Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention), Official Journal, L 271 of 24.10.2000, pp. 1-3.

[26] ADAM, Alexandre (2006), "L'échange de données à caractère personnel entre l'Union européenne et les Etats-Unis: Entre soucis de protection et volonté de coopération", *Revue Trimestrielle du Droit Européen*, 42(3), juill.-sept., p. 434.

[27] 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, Official Journal of the European Communities, L 8, 12.1.2001, pp. 1- 22.

[28] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, known as the 'e-Privacy Directive'), Official Journal, L 201,pp. 37-47, 31.7.2002.

		Eurojust[29]	
	Council Regulation (EC) No 407/2002 (Eurodac)[30]		
	Second stage of consultation on data protection in employment		
2003	ECJ Judgement Joined Cases C-465/00, C-138/01 and C-139/01 (Österreichischer Rundfunk and Others)[31]		
		Greek presidency proposes rules for third pillar data protection[32]	
	ECJ Judgement Case C-101/01 (Lindqvist)[33]		
2004	Draft Constitutional Treaty Article II-67: right to privacy. Article II-68: right to data protection[34] Data protection mentioned in Title VI on the democratic life of the Union		
	EC concludes PNR agreement with US[35]		
2005	i2010 Strategy Framework as part of the Renewed Lisbon Strategy		
		EC develops Hague Programme,[36] introduces the 'principle of availability'[37]	
			Signature of the **Prüm Treaty**[38]
	EC proposes legislation for SIS II[39]		

[29] Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, Official Journal, L 63, 6.3.2002, pp. 1-13.

[30] Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, Official Journal, L 62, 5.3.2002, pp. 1–5.

[31] 20 May 2003.

[32] In June 2003. EC (2006), Fact Sheet on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of judicial and police cooperation in criminal matters, SCADPlus, updated 31.3.2006.

[33] 6 November 2003.

[34] Treaty establishing a Constitution for Europe, Official Journal of the European Union, 2004/C 310/01, pp. 1-474.

[35] 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, Official Journal of the European Union, 6.7.2004, L 235, pp. 11-22, and Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, Official Journal of the European Union, L 183, 20.5.2004, pp. 83-85.

[36] European Council (2005), *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, Official Journal of the European Union, C 53, 3.3.2005, pp. 1-14.

[37] EC (2005), Communication from the Commission to the Council and the European Parliament. The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice, COM(2005) 184 final, 10.5.2005, Brussels.

[38] Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, Prüm, 27 May 2005.

		EC presents Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[40]	
2006	**Directive 2006/24/EC** (the 'Data Retention Directive')[41]		
	ECJ judgement Joined Cases C-317/04 and C-318/04, Parliament v. Council (PNR judgement)[42]		
			Conference of European Data Protection Authorities launches Working Party on Police and Justice
2007		As discussions on the Proposal for a Council Framework Decision reach deadlock at the Council, German presidency works on new version	
	Reform Treaty[43] Charter of Fundamental Rights adapted[44]		
	EC introduces proposal to amend Directive 2002/58/EC[45]		

2.2. The Right to Data Protection as an Autonomous Fundamental Right

The gradual recognition and development of the fundamental right to the protection of personal data[46] at EU level can be described as the result of a typically European process of reciprocal influences

[39] On 31 May 2005. The proposals were to become: Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Official Journal of the European Union, L 381, 28.12.2006, pp. 4-22 (known as Regulation on aspects of the SIS II first pillar); Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, Official Journal of the European Union, L 381, 28.12.2006, pp. 1-3; and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Official Journal of the European Union, L 205, 7.8.2007, pp. 63-81 (known as the Decision determining aspects of the SIS II third pillar).

[40] On 4 October 2005.

[41] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13.4.2006, pp. 54-63.

[42] Judgement of the Court (Grand Chamber) of 30 May 2006, *European Parliament v Council of the European Union*, Joined Cases C-317/04 and C-318/04 (2006/C 178/02), Official Journal of the European Union, C 178, 29.7.2006, p. 1–2.

[43] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, Official Journal, 2007/C 306 Vol. 50.

[44] Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 303, 14.12.2007, pp. 1-16.

[45] Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating and electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, 2007/INFSO/001, 13 November 2007.

[46] Generally referred to as the 'right to data protection'.

between national[47] and supranational legal frameworks.[48] In this process, Council of Europe legal instruments and the case law of the European Court of Human Rights (ECtHR) have played an especially relevant role. However, whereas the ECtHR has tended to widen the scope of the right to privacy as to make it cover the scope of the right to the protection of personal data, the fundamental right to the protection of personal data has been progressively configured at EU level as an autonomous, distinct right, independent from the right to privacy.

The inclusion of the right to the protection of personal data in the European Charter of Fundamental Rights,[49] in its Article 8, has been the major step for its recognition as an autonomous, independent fundamental right.[50] The content of Article 8 of the Charter was officially inspired in Community Law (especially, in Article 286 TCE and in the Data Protection Directive) and in Council of Europe instruments [both Article 8 of the European Convention on Human Rights (ECHR) and Convention No. 108].

The consecration of the right to data protection as an autonomous fundamental right was expected to be reinforced by the approval of the draft Constitutional Treaty, to render binding the EU Charter. The draft Constitutional Treaty reproduced in Article II-68 the content of Article 8 of the Charter. Moreover, Article I-51 of the draft Constitutional Treaty partially mirrored Article 286 of the Treaty and established the right to data protection in the general context of the EU institutions,[51] allowing for the adoption of instruments not limited to the Community area as under the mentioned Article 286.[52] As the constitutional project was eventually let aside and replaced by discussions on the Reform Treaty (Treaty of Lisbon, signed on 13 December 2007), expectations for a reinforced consecration of the right to data protection as a fundamental could be broadly maintained. The Reform Treaty should introduce as Article 16 B of the Treaty on the Functioning of the EU the content of current Article 286. The Lisbon Treaty furthermore foresees as Article 6 TEU on the recognition of the rights, freedoms and principles set out in the Charter.[53]

Article 8 of the EU Charter of Fundamental Rights, on the protection of personal data, reads as follows:

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

[47] Member States recognise the existence of a right to data protection in different ways. While some mention it in their constitutional texts (for instance, Portugal, Austria and Finland), others have recognised its existence through case law (most notoriously, Germany).

[48] ARENAS RAMIRO, Mónica (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia: Tirant Lo Blanch, p. 38.

[49] Hereafter, 'the Charter'.

[50] For a critical reading of the content of the right to the protection of personal data as presented in the Charter, see: RUIZ MIGUEL, Carlos (2003), "El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico", *Revista de Derecho Comunitario Europeo*, Año 7, Número. 14, Enero-Abril, p. 41.

[51] The final content of Article I-51 of the draft Constitutional treaty was however criticised for being more limited in scope than originally foreseen, especially for referring only to "*individuals"* [GUERRERO PICÓ (2005), "El derecho fundamental a la protección de datos de carácter personal en la Constitución Europea", *Revista de Derecho Comunitario Europeo*, n° 4, Julio-Diciembre, pp. 325-329].

[52] European Commission (2007), Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, 7.3.2007, Brussels, p. 8.

[53] The Charter was amended in 2007 and solemnly declared by the heads of the European Parliament, Council and Commission in the European Parliament 12 December 2007: Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 303, 14.12.2007, pp. 1-16.

has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Article 8 sets forth positive rights for the individual (right of access, right to rectify) and establishes obligations for those processing personal data (lawful processing). It has also a distinctive feature strongly influencing its legal development and implementation: it foresees the existence of special authorities entrusted to ensure compliance. These bodies, generally known as 'data protection authorities' or 'supervisory authorities', have been historically the main driving force pushing for the recognition of the right to data protection as an autonomous, fundamental right in the EU. Representatives of data protection authorities were already influential during the first drafting of the Data Protection Directive,[54] which represented a major breakthrough for data protection in the EU and is generally regarded as a remarkable example of promotion of fundamental rights policies in the name of internal market concerns.[55] Key actors from the community of data protection authorities were also strategically placed in the decision-making process to influence the very inclusion of the right to data protection in the 2000 Charter, as well as the reference to their existence at the heart of the right.[56] The consecration of the data protection right in the EU Charter of Fundamental Rights can also be explained by the role played by the representatives of national data protection authorities acting in the institutional framework of the Working Party on the Protection of Personal Data (the 'Article 29 Working Party'), which had been established by the Data Protection Directive.[57]

2.3. Asymmetries and apparent inconsistencies

Despite the general tendency to build the right to the protection of personal data as an autonomous fundamental right with EU-wide recognition and an increasingly large scope, a series of contrasted developments have been taking place. The implementation of the right has been highly contrasted in the first and the third pillars of the EU: while a series of instruments have ensured a consistent approach for data protection in the context of the first pillar, the third pillar has been systematically excluded from them.[58]

The first major legislative development of the right to data protection in Community law (the approval of the Data Protection Directive in 1995) marked already the path for an asymmetric development. The EC had accepted to support the initiative justifying it as a requirement for the construction of the internal market. Thus, it proposed the Data Protection Directive to be adopted with Article 100a of the

[54] Privacy and data protection interests were notably represented by Spiros Simitis, Chairman of the Commission's drafting group, Chair of the Council of Europe's Data Protection Experts Committee, and Hesse's Data Protection Commissioner [HEISENBERG, Dorothee (2005), *Negotiating Privacy: the European Union, the United States and Personal Data Protection*, London: Lynne Rienner Publishers, p. 62].

[55] EU Network Of Independent Experts On Fundamental Rights (2003), Report on the Situation of Fundamental Rights in the European Union and its Member States in 2002, 31 March, p. 15.

[56] The President of the Convention responsible for the preparation of the Charter was the German constitutionalist Roman Herzog, member of the German Federal Constitutional Court when such Court configured the right to self-determination as an autonomous right, a jurisdictional development with a strong impact on the conceptual development of the right to the protection of personal data [ARENAS RAMIRO, *op. cit.*, p. 244].

[57] In particular, the Chairman of the Article 29 WP at the time, Stefano Rodotà, is believed to have played an essential role in the adoption of Article 8 of the Charter (POULLET, Yves and Serge GUTWIRTH, "The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?", forthcoming, p. 14).

[58] For more details on data protection decision-making in the third pillar, see: GONZÁLEZ FUSTER, Gloria and Pieter PAEPE (2008), "Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects" in GUILD, Elspeth and Florian GEYER (eds.), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, pp. 129-150.

Treaty of Rome (currently Article 95 of the Amsterdam Treaty) as legal basis. The Data Protection Directive explicitly excluded from its scope of application processing related to matters falling under the third pillar.[59] Subsequent first pillar legal texts, such as Directive 2002/58/EC, were to bear the same scope limitation.[60] Although provisions on the protection of personal data in the third pillar do exist, they are all limited in scope,[61] and their impact cannot be compared to the far-reaching effect of the Data Protection Directive. The lack of uniformity amongst third pillar data protection provisions, moreover, is believed to translate into a series of disparities not always justified.[62] Over the years there have been many calls to put an end to this unbalanced situation. There have been specific calls for a EU-wide harmonizing approach (covering both the first and the third pillar),[63] as well as calls for provisions that would uniform protection in the third pillar.

Those supporting a more consistent development of the right to data protection in the EU have generally welcomed all institutional developments that could reduce the specificity of decision-making for matters falling under the third pillar.[64] Changes announced by the Reform Treaty were celebrated in this sense, as it is expected to widen the scope of matters falling under the co-decision procedure. However, it has also been argued that the Treaty of Lisbon may not reduce the specificity of EU justice and home affairs, but rather increase it.[65] The impact of the widening could be ultimately limited for data protection purposes, as, in accordance with the Reform Treaty, the European Parliament (EP) is only to be consulted on all *"measures concerning passports, ID cards, residence permits and any other such document",* which could include measures related to databases.[66]

---

[59] Art. 3.2 of Directive 95/46/EC exempts from its scope data processing occurring "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, defense, 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".

[60] In Article 1.3: "This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law".

[61] Specific rules on data protection were notably established for the Schengen Information System (SIS) already before the approval of the Data Protection Directive [see Articles 102-118 and 126-130 of the Convention implementing the Schengen Agreement of 14 June 1985]. It shall be pointed out that when no EU provisions on the protection of personal data are applicable, other international provisions might be relevant. The Convention implementing the Schengen Agreement of 14 June 1985 explicitly mentions as a complementary legal references to be taken into account the Council of Europe Convention 108 and Recommendation No R(87) 15 of 17 September 1987 [Article 115(1) of the Convention implementing the Schengen Agreement]. The 1995 CIS Convention [Article 18(2) of the CIS Convention] and the Europol Convention refer [Article 14(1) of the Europol Convention] to the same texts.

[62] For examples, see: GEYER, Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, Research Paper No. 9, CEPS, Brussels, May, p. 9.

[63] See for instance: Committee on Citizen's Freedoms and Rights, Justice and Home Affairs of the European Parliament (2004), *Report on the First Report on the implementation of the Data Protection Directive (95/46/EC)* , Rapporteur: Marco Cappato, 15-0104/2004 EN, 24 February, p. 7: *"…in the long term, Directive 95/46/EC should be applied, following the appropriate modifications, to cover all areas of EU activity, so as to guarantee a high standard of harmonised and common rules for privacy and data protection*".

[64] In this sense, the EDPS celebrated the constitutional draft welcoming notably the further integration into EU's structure of police and judicial cooperation [HUSTINX, Peter J. (2005), "Data Protection in the European Union", *P&I*, pp. 62-65].

[65] MARTENCZUK, Bernd and Servaas VAN THIEL (eds.), *Justice, Liberty, Security: New challenges for EU external relations*, Brussels: VUB Press, p. 17.

[66] See: BUNYAN, Tony (2007), "EU: Cementing the European State – new emphasis on internal security and operational cooperation at EU level", Statewatch Bulletin, vol. 17, 3/4, October.

The recognition of the right to the protection of personal data was explicitly discussed during the revision of the draft Constitutional treaty that lead to the Reform Treaty. The special care to be taken with its status was highlighted in the Presidency Conclusions that launched the Reform Treaty.[67] A comment in the declarations accompanying the text of the Constitutional treaty had rendered explicit the obligation for EU institutions to take into account implications for national security when regulating the protection of personal data.[68] Article 16 B of the Treaty on the Functioning of the EU, which is expected to replace Article 286 under the Reform Treaty, explicitly foresees a similar consideration: "*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*".[69] Moreover, three Member States (UK, Ireland and Denmark) have been recognized the right to partly op-out from the mentioned Article 16 B. Opt-outs from the generalized binding nature of the Charter (or special interpretations of its content at Member State level)[70] might complicate further any assessment of the status of the right to data protection as a EU fundamental right.

Traditionally, the main force pushing against a uniform implementation of the right to data protection in the third pillar and, in general, at EU level, have been national governments. To counter their reluctance, many arguments have been advanced over the years. One of the main arguments used was found in the need to accompany the implementation of the 'principle of availability', a EU-principle systematising the exchange of law enforcement data between Member States that was supposed to be adopted by January 2008 in accordance with the EC development of the Hague Programme.[71] It was sustained that the principle was not dissimilar to recognising a 'free movement of data' in the third pillar and that harmonising rules on data protection were thus needed. This was the logic followed by the EC with the simultaneous presentation of a draft Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (third pillar data protection) and a legislative proposal on the 'principle of availability' in October 2005. However, the development of the 'principle of availability' as such was eventually disregarded by the Council. Member States finally opted to implement a sort of wide 'availability' of data without any pan-European principle by integrating into the EU legal framework a text previously negotiated by a limited number of national governments, known as the Prüm Treaty.[72] The Council

---

67 "*In Article 286 (personal data protection), as amended in the 2004 IGC, a subparagraph will be inserted stating that the rules adopted on the basis of this Article will be without prejudice to those adopted under the specific legal basis on this subject which will be introducied in the CFSP Title (the IGC will also adopt a declaration on personal data protection in the areas of police and judicial cooperation in criminal matters, as well as, where appropiate, specific entries in the relevant Protocols on the position of individual Member States clarifying their applicability in this respect)"* [Council of the European Union (2007), *Presidency Conclusions, Brussels European Council 21/22 June 2007,* 23 June, 11177/07, Brussels, p. 20].

68 See point 10 of the Declarations Concerning Provisions of the Constitution: "*Declaration on Article I-51: The Conference declares that, whenever rules on protection of persona data to be adopted on the basis of Article I-51 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter*". It is additionally recalled that the legislation presently applicable (i. e., Directive 95/46/EC) includes specific derogations in this regard" (Treaty establishing a Constitution for Europe, OJ 2004/C 310/01, p. 423).

69 See: Treaty of Lisbon, point 29. The envisaged Article 25a refers to the adoption of special provisions for the right to the protection of personal data falling under the scope of the Chapter on the Common Foreign and Security Policy.

70 House Of Lords, European Union Committee (2008), *The Treaty of Lisbon: An Impact Assessment,* 10th Report of Session 2007-2008, HL Paper 62, The Stationery Office, London, 13 March, p. 102.

71 The Hague Programme, which was approved by the European Council on 5 November 2004 and set out the EU's priorities in the field of justice and home affairs for the following five years, invited the Commission to present by the end of 2005 legislation to implement the 'principle of availability' that would be operational by 1 January 2008.

72 The Prüm Treaty is an agreement originally established between Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, signed on 27 May 2005 (*Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of*

Framework Decision on third pillar data protection was long discussed at Council level and finally suffered important limitations, notably regarding its scope (finally expected not to cover processing of data at national level).[73]

cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, Prüm, 27 May 2005*)*.

[73] Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (2007), Report on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation), Rapporteur: Martine Roure, A6-0205/2007, 24.5.2007, p. 42.

3. Actors

This section introduces the main actors involved in the law and policy-making of the right to the protection of personal data in the EU. Actors have been classified in two different categories depending on their institutional or non-institutional nature, even if the frontier between the two categories can sometimes be nebulous. Some of the institutional actors, even if 'institutionalised', have actually been created essentially to canalise input from non-institutional actors.

3.1. Institutional actors

3.1.1. Main EU Institutions

a) European Commission

The European Commission (EC) plays different roles regarding the right to data protection, the most important being possibly the preparation of legislative and policy proposals. From a policy perspective is currently of outmost importance the i2010 strategic framework for the information society and media policies, laying out broad policy orientations for the EC, launched in 2005.[74] Privacy and data protection are key elements of this strategic framework, which is structured around three priorities: the completion of a Single European Information Space; strengthening innovation and investment in Information and Communication Technologies (ICT) research; and achieving an Inclusive European Information Society. The EC envisaged working for these aims reinforcing dialogue with stakeholders and working with Member States, "*notably through the open method of coordination".*[75] The EC has also specific duties as guardian of the Treaties, which can lead to action being taken against Member States. For instance, on 11 January 2000, it took five Member States[76] to the European Court of Justice (ECJ) for failure to implement the Data Protection Directive.

The main EC services dealing with data protection on a regular basis are the Data Protection Unit of Directorate-General Justice, Freedom and Security (DG JLS),[77] broadly responsible of issues related to the Data Protection Directive, on the one hand, and various services of the Information Society and Media Directorate-General (DG INFSO), which deal with data protection and privacy on different grounds in the context of the i2010 initiative, and notably responsible for the e-Privacy Directive, on the other hand. The EC and all other community bodies need to comply with the data protection provisions of Regulation (EC) No 45/2001 (see notably Section 3.1.7. on data protection officers).

Data protection legislation imposes on the EC specific tasks and grants it special powers. By virtue of the Data Protection Directive, the EC enjoys a privileged role in the determination of the third countries identified as providing 'adequate protection', which allows for the simplification of data transfers to the

---

[74] EC (2005), *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "i2010 – A European Information Society for growth and employment"*, COM(2005) 229 final, Brussels, 1.6.2005.

[75] *Ibidem*, p. 12.

[76] France, Germany, Ireland, The Netherlands and Luxembourg. Most of them reacted immediately and the required legislation came into force.

[77] The Data Protection Unit appeared in March 2005 in DG JLS following the EC decision of February 2005 to transfer the responsibility for its activities in this field from the Commissioner for the Internal Market, Charlie Mc Creevy, to Vice President Franco Frattini, Commissioner in charge of Justice, Freedom and Security. The Unit reference is C5, and it is part of Directorate C "Civil justice, fundamental rights and citizenship'".

third countries in question. Directive 99/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity allows the EC to decide, in accordance with a 'comitology' procedure, that certain apparatus shall be constructed incorporating safeguards ensuring that the personal data and privacy of the user and of the subscriber are protected.[78]

When the EC determines the need for action in a particular field, very different policy initiatives are at its disposal, ranging from top-down regulation to other, much more flexible approaches. For instance, the EC observed that the implementation of the Data Protection Directive in the health care sector in Member States might need further improvement.[79] To this effect, it simply offered to work with the Member States to raise awareness on the subject.[80] It shall be also stressed that regulation is not the only tool in the hands of policy-makers to promote the effective implementation of the right to data protection: specific non-legal solutions such as self-regulatory instruments and the promotion of so-called Privacy Enhancing Technologies (PETs)[81] are other possible tools generally discussed.

b) Council

The Council is generally portrayed as reticent to the adoption of proposals reinforcing the right to the protection of personal data at EU level. Discussion on issues related to data protection can take place internally in different working parties, generally not fully dedicated to the promotion of said fundamental right. A recent Council Working Party on Data Protection has enjoyed only an intermittent existence.[82] The European Council has played a key role in accelerating legislative and policy initiatives related to issues with potential negative effects on the right to privacy and data protection, such as the use of biometrics, the development of information systems and enabling exchanges of information, in particular through the multi-annual programme on Freedom, Security and Justice known as the Hague Programme.

c) European Parliament

Data protection had been the subject of debates and resolutions in the European Parliament (EP) already more than a decade before the EC introduced its first regulatory draft on the subject. The EP

[78] Article 3(3)(c) of Directive 99/5/EC. This possibility has not yet been used by the EC [EDPS (2007) Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007)96, 20 December, Brussels, p. 11].

[79] In COM(2004)301.

[80] HERVEY, Tamara (2006), *The European Union and the Governance of Health Care*, Paper presented at the annual meeting of the The Law and Society, J.W. Marriott Resort, Las Vegas, October, pp. 14-15.

[81] The EC has already manifested its support for wider use of PETs; see: EC (2007), Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, 2.5.2007, Brussels, p. 4. In particular, the EC has announced its intention to encourage "various stakeholder groups" to debate about them, adding that "[t]hese groups will include in particular representatives from the ICT sector, PETs developers, data protection authorities, law enforcement bodies, technology partners including experts from relevant fields, such as e-Health or information security, consumers and civil rights associations. These stakeholders should regularly look into the evolution of technology, detect the dangers it poses to fundament rights and data protection, and outline the technical requirements of a PETs response. This may include fine-tuning the technological measures in accordance with the different risks and the different data at stake and taking into account the need to safeguard public interests, such as public security" [ibidem, pp. 5-6].

[82] The 2006 Austrian Presidency convened two meetings of the working party. The Finnish Presidency convened a third meeting during the autumn of 2006 [EDPS (2007), *Annual Report 2006*, Office for Official Publications of the European Communities, Luxembourg, p. 55].

is currently regularly involved in the law and policy-making related to the protection of personal data through the normal institutional procedures. It also plays a role in raising awareness on data protection issues outside the framework of legislative procedures. For instance, it has recently called on the EC to ensure better protection of the citizen in digital environments.[83]

Even if some argue that reinforcing the involvement by the EP in decision-making can contribute to stronger consideration of data protection concerns,[84] the empirical data supporting such a view is limited. The specific impact of the different EU legislative procedures in the outcome of data protection legislation is indeed unclear. The Data Protection Directive was initially to be approved by the co-operation procedure. In 1993, the Directive became subject to the co-decision procedure, in principle granting the EP more decision-making power. In practice, the change from co-operation to the co-decision procedure is however believed to have been unimportant to the Directive's success.[85] Additionally, the EP plenary approved the controversial Data Retention Directive under co-decision procedure in December 2005.

The EP Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) launches regularly initiatives to follow developments considered relevant. It generally welcomes and supports the views of representatives from data protection authorities,[86] and has often echoed concerns previously expressed by the Article 29 Working Party or the European Data Protection Supervisor.[87] It is also a privileged interlocutor of the 'civil society' in this field.[88]

d) European Court of Justice

The European Court of Justice (ECJ) has contributed through its case law to the clarification of EU provisions on the right to data protection. Two judgements, the *Österreichisches Rundfunk* case[89] and the *Lindqvist* case,[90] have given to the ECJ the opportunity to assert that the non-application of the Data Protection Directive should represent an exception to be considered narrowly.[91] Interestingly, in

[83] EP (2007), European Parliament resolution of 21 June 2007 on consumer confidence in the digital environment (2006/2048(INI)), 21 June, Strasbourg, p. 9.
[84] HUSTINX, Peter (2008), *Strategic challenges for data protection in Europe*, speech delivered at the 9th Data Protection Conference, 6 May, Berlin, p. 6.
[85] HEISENBERG, *op. cit.*.
[86] For instance, the LIBE Committee organised a Public Seminar titled "*PNR/SWIFT/Safe Harbour: Are transatlantic data protected?: Transatlantic relations and data protection*" was celebrated in Brussels on 26 March 2007.
[87] See for instance: EP (2008), Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs, for the Committee on the Internal Market and Consumer Protection on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation(EC) No 2006/2004 on consumer protection cooperation, Rapporteur: Alexander Alvaro, 18.4.2008, p. 4.
[88] As an example of 'civil society' organisation addressing the LIBE Committee, Standing Committee Of Experts On International Immigration, Refugee And Criminal Law (Commissie Meijers) (2008), *Note to the Civil Liberties, Justice and Home Affairs Committee of the European Parliament regarding Views on the Commission report on the evaluation and future developmnet of the FRONTEX agency (COM(2008) 67 final)*, 4 April.
[89] Joined Cases C-465/00 (Rechnungshof v. Österreicher Rundfunk) and C-138/01 and C-139/01 (Neukomm and Lauermann v. Österreichischer Rundfunk). Complete references of case law mentioned can be found at the end of the report.
[90] Case C-101/01 (Göta hovrätt v. Bodil Lindqvist).
[91] POULLET, Yves (2006), "The Directive 95/46/EC: Ten years after", *Computer Law & Security Report*, 22, p. 211.

the conclusions for both cases, the Advocate General had manifested the view according to which the situations that were being examined felt outside the scope of application of Directive 95/46/EC.

Moreover, the ECJ in *Rechnungshof v Österreichischer Rundfunk and others* held that the provisions of the Directive must be interpreted in the light of fundamental rights, in particular the right to privacy, guaranteed by the EU. As a consequence, Article 8(2) of the ECHR is directly relevant for the interpretation of the Directive and national implementation measures.[92]

e) European Economic and Social Committee

The European Economic and Social Committee (EESC) regularly expresses opinions related to the right to data protection and the right to privacy.[93] The impact of such opinions is however modest, mainly because of the reduced relevance of the EESC in the EU decision-making process in general terms.

3.1.2. National and Sub-National Data Protection Authorities

Data protection authorities saw the light in Europe in the 1970s. Since then, they have multiplied and have gained recognition in different national and international legal instruments.[94]. The first EU legal instrument establishing the obligation for Member States to set up a data protection authority was the 1990 Schengen Convention implementing the Schengen Agreement of 14 June 1985. This Convention foresees the designation by each Contracting Party of a 'supervisory authority' responsible for carrying out independent supervision of the data in the national sections of the Schengen Information System (SIS) and for checking that the processing of data in SIS does not violate the rights of the data subject.[95] The 1995 Convention bears an equivalent disposition.[96]

The Data Protection Directive went a step ahead, confirming the need for all Member States to set up such authorities and providing minimum requirements for their design. By virtue of Directive 95/46/EC, each Member State might establish as many supervisory authorities as considered necessary. The e-Privacy Directive enlarged the tasks of data protection authorities to cover its scope. Other EU-related obligations for national and sub-national data protection authorities derived from the CIS and Europol regulations, which foresee that Member States grant certain rights to individuals through their supervisory authorities. A number of Member States have further extended the scope of their duties through implementing legislation.

---

[92] ANDENAS, Mads, and Stefan ZLEPTNIG (2003), "Surveillance and Data Protection: Regulatory Approaches in the EU and Member States", *European Business Law Review,* Vol. 14, n°6, p. 779.

[93] For instance, it expressed that the provisions of the proposal for the Data Retention Directive infringed fundamental rights. See: European Economic and Social Committee (2005), *Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* [(COM(2005) 438 final — 2005/0182 (COD)], Official Journal C 069 , 21/03/2006, pp. 16-21.

[94] The need for a supervisory authority has been internationally recognised by the United Nations in principle eight of the Guidelines for the Regulation of Computerised Personal Data Files, adopted by resolution 45/95 of the General Assembly on 14 December 1990, and by the 2001 Additional Protocol of Convention 108 of the Council of Europe of 1981. The need for data protection authorities as a principle is rarely questioned [for a defence of their relevance, see: FLAHERTY, David H. (1989), *Protecting Privacy In Surveillance Societies,* Chapel Hill: University of North Carolina Press].

[95] Article 114 of the Convention implementing the Schengen Agreement of 14 June 1985.

[96] Article 17 of the CIS Convention.

The supervisory authorities are, by virtue of the Data Protection Directive, to act independently.[97] There are however no EU level provisions on how to assure such 'independence'.[98] The vagueness of the Data Protection Directive on this point has not been an obstacle for the EC to launch infringement procedures against Member States[99] for not ensuring the independence of their respective authorities. The EC has actually identified independence of the authorities as one of its major concerns regarding the current implementation of Directive 95/46/EC,[100] stating that *""[t]hese authorities are key building blocks in the system of protection conceived by the Directive, and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation".*[101] The EDPS believes that the EC should monitor more effectively the compliance of Member States with the Data Protection Directive concerning the independence of supervisory authorities.[102] A case is currently still pending at the ECJ on divergent interpretations of a specific aspect to this notion.[103]

Not all supervisory authorities are granted the same powers by national administrations. Many enjoy regulatory competences and can adopt provisions favouring a uniform application of the law. It is the case, for instance, of the Greek, the Polish and the Slovak authorities.[104] Some data protection authorities enjoy audit powers, while others do not.[105] Information flows between governments and national data protection authorities seem to vary greatly dependent on the Member States, notably on governmental negotiations of EU information systems.[106] It has been pointed out that the practices

[97] Article 28 (and Recital 62) of Directive 95/46/EC.

[98] The Data Protection Directive simply states that the authorities must be able to "*act with complete independence in exercising the functions entrusted to them*" (Art. 28.1 of Directive 95/46/EC). In other words, *"[a]s regards the composition of the supervisory authorities entrusted with monitoring the application of the provisions adopted by the Member States, Directive 95/46/EC lays down that those authorities shall perform their tasks in complete independence. However, the Directive does not provide any further indication on the manner in which that independence must be ensured"* [BOLKENSTEIN, Frits (2002), *Answer on behalf of the European Commission dated from 26/09/2002 to:* "Written Question E-1723/02 by Bart Staes (Verts/ALE) to the Commission. The protection of privacy and electronic data processing", OJ C 052 E, 06/03/2003, p. 97].

[99] Austria (after a complaint from the data protection association Arge Daten introduced in October 2003 concerning the role of the Chairwoman of the Austrian Data Protection Commission, who was at the same time Head of the Data Protection Department at the Federal Chancellery) and Germany (following a complaint introduced by legal scientist Patrick Beyer concerning provincial Supervisory authorities) [EDRI-Gramm (2005), "EC: data protection inadequate in Austria and Germany", *EDRI-GRAMM Newsletter*, Number 3.17, 24 August, (retrieved from: http://www.edri.org/edrigram/number3.17/DPA)].

[100] EC (2007), Communication to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, (COM(2007) 87 final), Brussels, 7.3.2007.

[101] *Ibidem*, p. 5.

[102] EDPS (2007), Opinion on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 25 July, Brussels, p. 7.

[103] Action brought on 22 November 2007, Commission of the European Communities v Federal Republic of Germany (Case C-518/07).

[104] ARENAS RAMIRO, *op. cit.*, p. 566.

[105] The UK data protection authority, for instance, does not have audit powers, despite calls in this direction (House Of Lords, European Union Committee (2005), *European Union: Fifth Report*, European Union Committee Publications, Session 2004-2005, 22 February, point 105).

[106] For instance, the German data protection authority has been is recurrently informed and consulted on SIS II, while the one from the UK has not [House Of Lords, European Union Committee (2007), *Schengen Information System II (SIS II), Report with evidence,* 9th Report of Session 2006-2007, HL Paper 49, 2 March, The Stationery Office, London].

developed by data protection authorities are substantially dependent on the powers and mechanisms with which they are equipped.[107]

The relation between data protection authorities and the population consists primarily in the reception and management of complaints. Some national and sub-national authorities have also other procedures to obtain input from the population, and they sometimes launch consultation procedures at national level on subjects related to data protection.[108] Certain data protection authorities engage actively in awareness-raising campaigns.[109] The relation with 'civil society' representatives is not always pacific, as some organisations believe that data protection authorities fail to effectively protect the right to privacy and the protection of personal data.[110]

According to the last Eurobarometer survey, only 28% of EU citizens interviewed affirmed that they had ever heard about the existence of a data protection authority in their country. Seven out of 10 respondents were not aware of the existence of such an authority in their country.[111] Levels of awareness ranged from 15% in Bulgaria to 51% in Greece, 46% in Hungary. The general lack of awareness has basically remained unchanged at EU level over the last five years, despite some different evolutions at national level.[112]

The perception of data protection authorities of their own role regarding the development of the right to data protection can differ strongly from one authority from the other, and can also be different amongst the members of a same authority. Such self-perception can range from a vision of data protection authorities as strict supervisors of legal compliance to a larger notion of bodies entrusted with a responsibility to proactively promote the right to data protection.[113] Illustrating the proactive approach, a group of national data protection authorities supported by the EDPS are developing since November

---

[107] Article 29 Working Party (2006), Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the e-Privacy Directive, WP 126, 26 September.

[108] For instance, the French data protection authority (Commission Nationale de l'Informatique et des Libertés, CNIL) organised between November 2006 and February 2007 more than 60 auditions to obtain evidence on the issue of "measures of diversity" from the civil society, trade unions, private companies, universities and research centres, as well as religious representatives. An on-line questionnaire was also used. See: Commission Nationale De L'informatique Et Des Libertés (CNIL) (2007), *27e Rapport d'activité 2006*, La Documentation Française : Paris, p. 69.

[109] For example, the Norwegian Data Protection Authority and the Portuguese Data Protection Authority have recently engaged in campaigns aimed at the young people [International Working Group on Data Protection in Telecommunications (2008), *Report and Guidance on Privacy in Social Networks Services, 'Rome memorandum'*, 43rd Meeting, 3-4 March 2008, Rome, P 10].

[110] For instance, on 14 December 2007, a group of persons occupied the building of the French data protection authority to protest against its limited actions to counter surveillance. The action was supported by a series of associations such as: Groupe Oblomoff, Pièces et Main d'Œuvre, Mouvement pour l'Abolition de la Carte d'Identité (MACI), Halte aux puces!, Coordination contre la biométrie, Souriez, vous êtes filmés! (more information at: http://juralibertaire.over-blog.com/article-14607456.html). For a view of civil society organisations' recurrent demands to data protection authorities, see: *Declaration of Civil Society Organizations On The Role of Data Protection and Privacy Commissioners*, Montreal, 25 September 2007 [signed by European Privacy Information Center, European Digital Rights, Privacy International, Statewatch and others].

[111] Gallup Organization (2008), *Data Protection in the European Union: Citizens' perceptions*, Analytical Report, Flash Eurobarometer 225, February, p. 34.

[112] *Ibidem*, p. 35.

[113] The Article 29 Working Party has stated, for instance, that "*the role of data protection authorities is four-fold: to educate and inform (…); to influence policy makers to make the right decisions (…); to make controllers aware of their duties; and to use their powers against those who disregard legislation or do not adhere to codes of conduct or best practice…*" [Article 29 Working Party (2008), *Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)*, WP 147, 18 February, p. 18].

2006 the so-called 'London initiative', aimed at 'communicating data protection and making it more effective'.[114]

3.1.3. The Article 29 Working Party

The Data Protection Directive created the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, generally referred to as 'the Article 29 Working Party',[115] as a consultative independent body composed of representatives of national data protection authorities. The EDPS is one of its members and has the right to vote; the EC can participate, but without voting, and provides the secretariat. The main task of the Article 29 Working Party is to advise the EC on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data.[116] By virtue of Article 30(6) of Directive 95/46/EC, the Working Party has the obligation to "*draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council*". The report shall be made public.

The Article 29 Working Party was originally envisaged as a tool to lead to a more harmonized approach to data protection within the EU, making it less likely that individual Member States implement legislation in substantially divergent ways.[117] The Working Party's pronouncements and opinions can have significant impact on national supervisory authorities, as well as on national courts.[118] The body also contributes to the widespread of EU level concerns amongst national authorities, and favours the dissemination of information coming from national and sub-national data protection authorities amongst all the authorities involved. Coordinated European inquiries are sometimes launched in its framework.[119]

The Article 29 Working Party has played a very relevant role as an instrument allowing data protection authorities *as a community* to define, voice out and support their own agenda on the right to data protection in general at EC level.[120] However, its competencies are limited to the first pillar, and do not reach third pillar decision-making. The Article 29 WP has sometimes used its consultative powers to

---

[114] On the 'London initiative' and other data protection authorities' recent efforts for the improvement of enforcement, see: TREACY, Bridget (2008), "Enforcement: EU Data Protection", *Privacy & Security Law*, Volume 7, Number 12, 24 March, pp. 439-442.

[115] The e-Privacy Directive widened the scope of activities of the Article 29 Working Party [see Article 15(3)].

[116] The Article 29 Working Party has the obligation to advise the Commission on any eventual amendment of the Data Protection Directive, as well as the right to make recommendations on its own initiative on "*on all matters relating to the protection of persons with regard to the processing of personal data in the Community" (*Art. 30.3 of Directive 95/46/EC). This right has been interpreted largely with the argument that no data protection provision in the EU shall be considered completely unrelated to first pillar data protection.

[117] KUNER, Christopher (2003), *European Data Privacy Law and Online Business*, New York: Oxford University Press, p. 32.

[118] *Ibidem*, p. 10.

[119] For instance, the Article 29 Working Party has investigated the health insurance sector across all Member States. National data protection authorities sent out written questionnaires to gather information from health insurance companies within their jurisdiction. This approach was considered the only way to collect consistent information across all Member States in the light of the diverse powers of each authority.

[120] Some researchers consider that the influence of data protection authorities on EU decision-making, canalised essentially through the Article 29 Working Party, is a key element differentiating 'governance' in this field. The term 'incorporated transgovernmentalism' has been suggested to describe this phenomenon of influence of national and sub-national independent authorities on supranational institutions [EBERLEIN, Burkard and Abraham NEWMAN (2008), *Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union*, Governance, vol. 21 (1), pp. 25-52].

recommend an increase of its own involvement in the decision-making process, occasionally next to the EDPS.[121]

3.1.4. Article 31 Committee

Article 31 of the Data Protection Directive establishes a 'comitology' procedure involving a committee that has come to be known as 'Article 31 Committee'.[122] It is composed of composed of representatives of the Member States and chaired by an EC representative.

3.1.5. European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) was established in 2001.[123] It is composed of a Supervisor and an Assistant Supervisor, both appointed by the EP and the Council on the basis of a list of candidates provided by the EC.[124] The members of the EDPS shall be chosen from persons "*who are acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities referred to in Article 28 of Directive 95/46/EC*".[125] The first Supervisor nominated had previously been chairman of a national authority, as well as chairman of the Article 29 Working Party. In his view, both the Article 29 Working Party and the EDPS "*defend the same substantial interests*".[126]

The EDPS has the obligation to publish an annual report to be submitted to all Community institutions and bodies and made public.[127] Contrary to the Article 29 Working Party, it can engage in legal proceedings related to matters falling under the scope of its tasks.[128] It structures its activities around three axes: supervision, consultation and cooperation.

a) Supervision

The EDPS is responsible for monitoring EC institutions' and bodies' compliance with their data protection obligations. It is notably involved in the supervision of the Customs Information System

[121] "The Article 29 Working Party should also be consulted in addition to the European Electronic Communication Market Authority and EDPS, since any measures introduced will directly affect the information to be given to persons concerned" [Article 29 Working Party (2008), Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), WP150, 15 May, p. 4].

[122] See Article 31 of the Directive 95/46/EC.

[123] For a detailed description of the EDPS, see: HIJMANS, Hielke (2006), "The European Data Protection Supervior: The Institutions of the EC Controlled by an Independent Authority", *Common Market Law Review,* 43, pp. 1313-1342.

[124] See Article 42.1 of Regulation (EC) No 45/2001.

[125] Article 42.2 of Regulation (EC) No 45/2001.

[126] European Data Protection Supervisor (2006), *Annual Report 2005*, p. 57.

[127] Article 48 of Regulation (EC) No 45/2001.

[128] In the PNR cases (Joined cases C-317-04 and C-318/04), the Court made an explicit reference to Article 41(2) of Regulation 45/2001, supporting the EDPS' reading according to which it is responsible for advising Community institutions and bodies on all matters concerning the processing of personal data. The EDPS has notably requested to intervene before the Court of Justice in the data retention case of Ireland vs. the Council and the European Parliament (Case C-301-06). Ireland claims that the Court should annul the Directive on the retention of communication data (2006/24/EC). The EDPS requests to intervene in support of the defendants, arguing that the case offers the possibility to clarify the Court judgement in the PNR-case. The key question concerns the applicability of Community law to the use of personal data collected by private companies for law enforcement purposes. According to the EDPS, a too limited interpretation of the scope of Community law in this respect would harm the protection of the individuals.

(CIS) database falling under Community law, and the Central Unit of Eurodac (database storing fingerprints of applicants for asylum).

The tools and mechanisms used for supervision purposes by the EDPS include 'prior checks', processing of complaints, inquiries, inspection policy and advice on administrative measures.[129] 'Prior checking' as a technique for supervision is mentioned in the Data Protection Directive[130], and can be conceptually related to the Privacy Impact Assessments (PIAs) foreseen in certain Member States for specific types of processing activities.[131] Just like PIAs, it is also based on the anticipatory consideration of potential impact on privacy and data protection of envisaged measures.

The supervision of Eurodac is globally operated by the Eurodac Supervision Coordinated Group, composed of the EDPS and representatives from the data protection authorities of the participating States. The EDPS is responsible of providing the secretariat to the Coordinated Group.[132] The EDPS is also to be involved is the supervision of the second generation of the Schengen Information System (SIS II). The idea of establishing coordinated supervision for SIS II was originally suggested by the EDPS itself in response to a request from the EP for advice on how to structure such supervision.[133] The EDPS later expressed concern for the supervision of SIS II for the transitional period during which the management of SIS II can be delegated by the EC to one or more Member States. This resulted in a special provision for the regulation on data protection during the transitional period, ensuring supervision by the EDPS.[134] The coordinated supervision model was later also to be considered for the Visa Information System (VIS), expected to become the largest biometric database in the world.

b) Consultation

In the name of 'consultation' the EDPS develops its advisory role, notably performed through the issuing of opinions on legislative proposals and related documents. The EDPS can advise Community institutions and bodies either on his own initiative or in response to a consultation,[135] and considers itself entitled to advise on all matters concerning the processing of personal data.

The EC must imperatively consult the EDPS when submitting certain legislative proposals. Article 28(2) of Regulation (EC) No 45/2001 establishes that the EC shall consult the EDPS "*when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data*". It then provides guidance publishing an opinion, most of the times globally supporting adoption and recommending improvements.[136] The EDPS is sometimes consulted by the EC even before the presentation of proposals, and reacts by providing informal comments.[137]

---

[129] EDPS (2008), *Annual Report 2007,* Brussels, p. 6.

[130] See Article 20 of Directive 95/46/EC.

[131] Linden Consulting, Inc. (2007), *Privacy Impact Assessments: International Study of the Application and Effects*, prepared for Information Commissioner's Office (United Kingdom), Loughborough University, October, p. 32.

[132] Eurodac Supervision Coordination Group (2007), *Report on the first coordinated inspection*, 17 July, Brussels. Supervision of Eurodac would initially be entrusted to a provisional Joint Supervisory Authority, replaced by the EDPS in January 2004.

[133] On January 2006.

[134] EDPS (2007), *Annual Report 2006*, Office for Official Publications of the European Communities, Luxembourg, p. 46-47.

[135] Article 46(d) of Regulation (EC) No 45/2001.

[136] In 2007 the EDPS concluded for the first time that a legal instrument, as proposed by the EC, should not be adopted; the opinion concerned a proposal for a Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes [EDPS (2008), *Annual Report 2007,* Brussels, p. 41].

[137] For instance, the EC informally consulted the EDPS on the draft prior to the adoption of the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC

Despite general compliance by the EC with its consultation obligations, the EDPS has already accused the EC of failing to comply.[138] Special attention has been given by the EDPS on to how to advise the EC in cases where it does not adopt a proposal but decides directly on an issue, as in such cases a formal opinion published after the adoption of a text cannot have any real influence on its content.[139] In 2007, the EDPS presented for the first time opinions on EC communications.[140] Although there is no legal obligation for a Member State taking the initiative for a legislative measure under Title VI of the EU Treaty to ask for advice, the EDPS has stressed that the procedure does not preclude the request for such advice either.[141] The EDPS has issued opinions on its own initiative in the cases in which it has considered appropriate to do so.[142] Regarding certain proposals, it has complained about the piecemeal way in which they are introduced, making it especially difficult for stakeholders to contribute meaningfully to the discussions. The EDPS has therefore called for evidence on the 'master plan' or overarching strategy underpinning certain series of measures.[143]

The EDPS sometimes uses its advisory position not only to protect and to promote the right to data protection as such, but also to promote an enhanced role for the EDPS in decision-making.[144] The

---

concerning the processing of personal data and the protection of privacy in the electronic communications sector. The EDPS was later glad to see that some of his suggestions have been reflected in the Proposal [EDPS (2008), *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, 10 April, p. 3].

[138] On 18 October 2007, the EC submitted a Proposal for Regulation to the European Parliament and the Council aiming at amending Regulation (EC) 2252/2004. The EDPS was not consulted about this proposal, on which he nonetheless decided to issue an opinion at his own initiative [EDPS (2008), *Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 26 March, Brussels, p. 1].

[139] EDPS (2007), *Annual Report 2006*, Office for Official Publications of the European Communities, Luxembourg, EN, p. 40.

[140] EDPS (2008), *Annual Report 2007*, Brussels, p. 41.

[141] EDPS (2008), Opinion of the European Data Protection Supervisor on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism, and cross border crime, Official Journal of the European Union, C 89, 10.4.2008, p. 1.

[142] Such as the initiative for a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, an the initiative with a view to adopting a Council Decision on its implementation.

[143] EDPS (2008), Preliminary Comments on Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union" COM(2008) 69 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final, 3 March, Brussels.

[144] For instance, in its opinion on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, the EDPS welcomes that the EC text explicitly establishes that prior to adopting implementing measures the EC will consult the EDPS [EDPS (2008), *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, 10 April, Brussels, p. 3].

EDPS sometimes advises systematic consultation of the EC with other stakeholders,[145] but does not systematically include under the 'stakeholders' tag 'civil society' representatives. For instance, the EDPS has manifested that improvements of the implementation of the Data Protection Directive cannot be achieved without the involvement of 'a broad range of stakeholders'. The main stakeholders cited in this occasion by the EDPS are however, besides data protection authorities and the Member States, private parties able to promote self-regulation and European Codes of Conduct, or to develop privacy-enhancing technologies.[146]

c) Cooperation

The EDPS has the duty to cooperate with other data protection authorities (both the national data protection authorities[147] and the joint authorities set up in the EU third pillar)[148] and the right to participate in the activities of the Article 29 Working Party. It also possesses special powers regarding EC data protection officers,[149] and has actively contributed to the definition of their practices and to the establishment and functioning of the network through which they collaborate. The EDPS cooperation rights and duties rights confer to the body a particularly privileged position in the EU decision-making process, which could be qualified as pivotal and strategic for the transfer of learning.

The EDPS has established good cooperation practices with the EP,[150] in particular with the LIBE Committee.[151] It is moreover devoted to intensifying its relations with the Council Presidency and the Council Secretariat, in particular with the aim of transforming into standard practice the presentation of EDPS opinions in Council Working Groups. Like the Article 29 Working Party, the EDPS has served as an instrument to promote at EU level the concerns of the community of data protection authorities.[152] Moreover, it has publicly stated that one of its main challenges is to develop a 'data protection culture' as part of 'good governance'.[153] While EDPS' coordination and integration with other institutional actors can be considered well advanced,[154] coordination with non-institutional actors (especially, 'civil society' representatives) is less developed and certainly not formalized.

---

[145] EDPS (2008), Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 26 March, Brussels, p. 3.

[146] EDPS (2007), Opinion on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 25 July, Brussels, p. 4.

[147] Article 46(f)(i) of Regulation (EC) No 45/2001.

[148] *Ibidem*, Article 46(f)(ii). This cooperation has translated for instance in participation of the EDPS as an observer in certain meetings.

[149] Article 24(1)(b) of Regulation (EC) No 45/2001.

[150] The EP notably played an effective role in amplifying EDPS views on VIS.

[151] EDPS (2006), *Inventory 2007*, December, Brussels, p. 4.

[152] A sign of the EDPS support to general concerns of the international network of data protection authorities is for instance the fact that on its site are posted a number of documents from the Conference of European Data Protection Authorities and from the International Conference of Data Protection and Privacy Commissioners, conferences in which he participates under his own notion of cooperation with EU data protection authorities in a 'wider context'.

[153] European Data Protection Supervisor (2007), *Annual Report 2006*, Office for Official Publications of the European Communities, Luxembourg, EN, p. 11.

[154] It should be added that the EPDS signed a Memorandum of Understanding with the European Ombudsman in November 2006. The European Ombudsman and the EDPS have overlapping competences in the area of complaint handling in the sense that instances of maladministration may concern the processing of personal data.

3.1.6. Joint Supervisory Authorities

Over the years, a series of EU level data protection supervisory bodies have been established in the third pillar. The SIS Joint Supervisory Authority, the CIS Joint Supervisory Authority and the Europol Joint Supervisory Authority share a common secretariat since 2001,[155] financially supported by the Council. Formal cooperation between these Joint Supervisory Authorities is not foreseen by any legal provision. Informal cooperation is however favoured by the fact that the same representatives can be implicated in different authorities. The Joint Supervisory Authorities do not have any formal contact with the Article 29 Working Party, even if they all have cooperation obligations vis-à-vis the EDPS. A meeting of "*representatives of those data protection authorities operating at EU level*"[156] was exceptionally celebrated once.[157]

The possibility of creating a common third pillar joint authority has been regularly discussed in many circles. In 2001, a draft resolution foresaw the possible existence of an authority common to all Member States.[158] In 2004, the European Conference of data protection authorities launched its own plan for the set up of a "*joint EU forum on data protection in police and judicial cooperation matters (data protection in the Third pillar)".*[159] The draft Constitutional Treaty originally foresaw the unification of all the different supervisory authorities operating at EU level, but the idea was finally removed.[160]

a) SIS Joint Supervisory Authority

The 1990 Convention implementing the Schengen Agreement of 14 June 1985 established a Joint Supervisory Authority consisting of two representatives from each national supervisory authority. The SIS Joint Supervisory Authority was set mainly as responsible for supervising the technical support function of SIS, but it was also granted the task of studying any problems that might occur regarding the exercise of independent supervision or the right of access to data held in SIS, and for drawing up harmonised proposals for joint solutions for existing problems.[161] The SIS Joint Supervisory Authority design has served as a model for the design of the other third pillar Joint Supervisory Authorities.[162]

b) CIS Joint Supervisory Authority

In 1995, the CIS Convention set up a Joint Supervisory Authority consisting of two representatives from each Member State drawn from their respective supervisory authority "*or authorities*".[163] The CIS

[155] Council Decision of 17 October 2000 already mentioned, Article 6(1).
[156] The EDPS, the chairs of Joint Supervisory Authorities and the chair of the Art. 29 WP.
[157] It was decided at the 2004 conference of European data protection authorities in Rotterdam.
[158] "Observance of the principles of personal data protection should be monitored and enforced by one or more independent public supervisory authorities of, or common to, the Member States" [Presidency of the Council (2001), Note 6316/2/01 JAI 13, From the Presidency to Article 36 Committee, "Subject: Draft Resolution on the personal data protection rules in instruments under the third pillar of the European Union", 12 April, Brussels, p. 10].
[159] A resolution calling for the creation of a joint EU forum on data protection in police and judicial cooperation matters was adopted in September 2004 by the European Data Protection Commissioners at a meeting held in Wroclaw, Poland.
[160] GUERRERO PICÓ, *op. cit.*, pp. 325-329.
[161] Article 115 of the Convention implementing the Schengen Agreement of 14 June 1985.
[162] BRULIN, *op. cit.*, p. 139.
[163] Article 18 of the CIS Convention.

Joint Supervisory Authority is competent to supervise the CIS database falling under the scope of the CIS intergovernmental convention,[164] to examine any eventual difficulties, to study problems which might arise with regard to the exercise of supervision by the supervisory authorities of the Member States, or in the exercise of rights of access by individuals, and to draw up proposals for the purpose of finding joint solutions to problems. Serious difficulties for the fulfilment of the CIS Joint Supervisory Authority tasks have derived from the fact that it does not possess a dedicated budget: it relies on the Council for financial assistance. The Council has been accused of recurrently refusing to fund inspections.[165]

c) Europol Joint Supervisory Body

Also in 1995, the Europol Convention draw up a Joint Supervisory Body composed of not more than two representatives of each of the national data protection supervisory bodies to ensure that the rights of individuals are not violated by the storage, processing or utilisation of data in its possession. In addition, the Joint Supervisory Body was allocated the task to monitor the permissibility of the transmission to third parties and third bodies of data originating from Europol.[166]

d) Eurojust Joint Supervisory Body

In 2002 a Joint Supervisory Body was created to monitor the protection of personal data with regard to Eurojust activities. It is composed of national representatives who must be judges not members of Eurojust or people holding an office giving them sufficient independence, when national systems require so.[167] The special nature of Eurojust is the reason behind the special nature of its Joint Supervisory Body.

3.1.7. Data Protection Officers

The Data Protection Directive mentions that Member States are entitled to regulate the existence of 'data protection *officials'*, understood as employees responsible for data protection working for data controllers.[168] The model of internal supervision of data protection compliance through in-house data protection officials has been increasingly praised over the years.[169] Until recently, however, only seven

[164] The CIS database falling under the scope of Community law is supervised by the EDPS.

[165] CIS Joint Supervisory Authority (2005), Opinion to the Council of the European Union on Supervising the Customs Information System, 4 March 2005, 7106/05, Brussels, p. 3.

[166] Article 24 of Europol Convention. On the transmission to third parties and third bodies, see Article 18 of Europol Convention.

[167] Article 23 of Eurojust Council Decision.

[168] See: Recital 49 of Directive 95/46/EC, where a reference is made to the possibility that "a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects", Art. 18.2 concerning the possible exemption of notification if a data protection official is in place, and Recital 54 and Art. 20.2, both concerning the possible implication of data protection officials in prior checks (according to Art. 20.2, data protection officials can be responsible of prior checking although "in case in cases of doubt, [they] must consult the supervisory authority").

[169] BENDRATH, Ralf (2007), *Privacy Self-Regulation and the Changing Role of the State: from Public Law to Social and Technical Mechanisms of Governance*, TranState Working Papers, No. 59, Sfb597, Staatlichkeit im Wandel / Transformations of the State, Bremen, p. 14.

Member States had established a national legislative framework for data protection officials,[170] and Germany was the only Member State rendering their appointment obligatory under certain circumstances.[171] In Italy they were established in the context of the regulation of biometrics.[172] In France, the model was introduced in 2004.[173] Data protection authorities have extensively been judged positive those national experiences.[174]

Regulation (EC) No 45/2001 established as a binding norm that each Community institution and body shall appoint a data protection *officer*, whose main function is to independently ensure the internal application of the aforementioned Regulation.[175] 'Data protection officers' must be independent[176] from the institution they work for, and they have the legislative obligation to cooperate with the EDPS. The EDPS found extremely useful in order to develop this cooperation the existence of an informal network of officers created by the officers themselves through regular meetings. In 2007, a 'quartet' composed of four data protection officers (from the Council, the EP, the EC and the Office of Harmonization for the Internal Market) was set up to coordinate the network.

The EC has appointed a special data protection officer for the European Anti-Fraud Office (OLAF) directorate-general, as well as a 'data protection coordinator' in each one of the other directorates-general.[177] The data protection officer model has also reached the third pillar. In 2002 it was established that Eurojust should have a specially appointed data protection officer.[178] Europol has also its own data protection officer, accepted into the informal network of officers working at EC institutions as an observer since 2007.

3.1.8. Other

a) EU Network Of Independent Experts On Fundamental Rights

Following a call of the EP, a Network of independent experts on fundamental rights was set up in September 2002. It consisted of one expert per Member State and headed by a coordinator. One of the main tasks it was allocated with was to assist the EC and the EP in developing the EU policy on fundamental rights. The Network has had the opportunity to express its views on the right to data

[170] Officials are sometimes referred to as "*chief privacy officers*", and can be organized in transnational professional organizations such as the International Association of Privacy Professionals (IAPP) or the European Privacy Officers Forum (EPOF) [*ibidem*, p. 15].
[171] KORFF, Douwe (2005), *Data Protection Laws in the European Union*, Richard Hagle, Belgium: Federation of European and Interactive Marketing, 2nd Edition, p. 149.
[172] In 2005, under the name of "*vigilatori dei dati*" [AGOSTINI, Aldo (2006), *Biometria e privacy: i presunti nemici a confronto - Guida Pratica,* Bologna: EDIS Edizioni Specializzate SRL, p. 30].
[173] Commission nationale de l'Informatique et Des Libertés (CNIL) (2007), *27e Rapport d'activité 2006*, La Documentation Française : Paris, p. 54.
[174] Working Party on the Protection Of Individuals with Regard to the Processing of Personal Data (2005), Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union, WP 106, adopted on 18 January, 10211/05/EN, p. 6.
[175] Article. 24.1 of Regulation (EC) No 45/2001.
[176] Article 24 of Regulation (EC) No 45/2001 provides a series of safeguards for independence, such as the need of consent from the EDPS to dismiss a Data protection officer (Art. 24.4).
[177] European Data Protection Supervisor (2007), *Annual Report 2006*, Office for Official Publications of the European Communities, Luxembourg, EN, p. 17.
[178] Who shall be a member of the staff taking instructions from no-one and who shall have the task of ensuring lawfulness and compliance with data protection provisions, as well as certain information tasks (see Article 17 of the Eurojust Council Decision).

protection in different occasions.[179] It has notably voiced out support for the use of the preventive monitoring[180] and the open method of coordination to promote fundamental rights in the EU.[181]

b) The European Union Agency for Fundamental Rights

The European Union Agency for Fundamental Rights was established in March 2007.[182] Its main tasks are the collection of information and data, research and analysis; to provide advice to EU institutions and Member States; and to co-operate with 'civil society'[183] and contribute to awareness raising. On 28 February 2008, the Agency's first Multi-Annual framework was adopted,[184] establishing that the Agency will work among others in the area of *"information society and, in particular, respect for private life and protection of personal data".*[185]

c) European Group on Ethics in Science and New Technologies

The European Group on Ethics in Science and New Technologies (EGE) is an independent body composed of fifteen experts appointed by the EC.[186] It examines ethical questions arising from science and new technologies and issues opinions to the EC in connection with the preparation and implementation of Community legislation or policies. Before issuing an opinion, the Group organises a roundtable to which representatives of EU institutions, other experts and parties representing different interests are invited to participate. The European Group on Ethics has taken into account privacy and data protection concerns in some of its opinions.[187] The Group is however not expected to deal with data protection issues in the near future, as it is for the time being busy with other, not directly related subjects.

d) European Network and Information Security Agency

The European Network and Information Security Agency (ENISA) was established to support the capability of Member States, EU-institutions and the business community to prevent, address and

---

[179] For instance, when Unit A5 of DG Justice and Home Affairs of the European Commission requested a thematic observation on the balance between liberty and security in the reactions form the EU and the Member States to the terrorist threads to the Network of Independent experts on fundamental rights. It was delivered on March 2003: Réseau UE d'experts Indépendants Sur Les Droits Fondamentaux (CFR-CDF) (2003), *L'équilibre entre liberté et sécurité dans les réponses de l'Union Européenne et de ses Etats membres à la menace terroriste,* Observation thématique, 31 mars.

[180] EU Network Of Independent Experts On Fundamental Rights (2003), Report on the Situation of Fundamental Rights in the European Union and its Member States in 2002, 31 March, p. 19.

[181] *Ibidem,* p. 25.

[182] Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, Official Journal of the European Union, L 53, 22.2.2007, p. 1–14.

[183] On cooperation with the 'civil society', see Article of Regulation (EC) No 168/2007.

[184] Council Decision of 28 February 2008 implementing Regulation (EC) No 168/2007 as regards the adoption of a Multi-annual Framework for the European Union Agency for Fundamental Rights for 2007-2012, Official Journal of the European Union, Official Journal, L 63, 7.3.2008, pp. 14–15.

[185] Article 2(h) of Council Decision of 28 February 2008.

[186] For the current mandate: Commission Decision of 11 May 2005 on the renewal of the mandate of the European Group on Ethics in Science and New Technologies (2005/383/EC), Official Journal of the European Union, L 127, 20.5.2005, pp. 17-19.

[187] See, for instance: European Group on Ethics in Science and New Technologies (2005), *Ethical aspects of ICT implants in the human body*, Rapporteurs: Stefano Rodotà and Rafael Capurro, adopted on 16 March.

respond to network and information security problems.[188] It has among its objectives to assist the EC in the technical preparatory work for updating and developing community legislation in the field of network and information security.[189] ENISA is assisted by a Permanent Stakeholders' Group with consultative tasks, composed of experts representing *"the relevant stakeholders".*[190] A 2007 report commissioned by the EC was very critical about ENISA, which is currently expected to be further sustained only in order to ease the handover to a new authority with wider powers.

e) European Security Research and Innovation Forum

The European Security Research and Innovation Forum (ESRIF) is a public-private partnership set up by the EC in September 2007[191] as a permanent forum of 50-70 members bringing together, on a voluntary basis, representatives of governments, industry, academics and 'civil society' to examine areas of research for public security needs.[192] ESRIF is expected to complement the EU legislation and funding programmes aiming to increase security for EU citizens, to help identify priority areas for standard-setting at EU level and to streamline security research activities in the EU. ESRIF shall present a Joint Security Research Agenda towards the end of 2009.

f) Expert Group on Radio Frequency Identification

The Expert Group on Radio Frequency Identification (RFID), sometimes referred to as 'the RFID-Stakeholder Group', was set up by the EC[193] in 2007 to operate between July 2007 and March 2009. Its members are described as representatives of end-user communities subjected to RFID systems [such as the European Consumers' Organisation, (BEUC)], of 'privacy organisations' [currently of only one 'privacy organisation', namely European Digitals Rights initiative, (EDRi)], of users from different application sectors, of industries actively involved in setting up RFID systems and of standardisation bodies. Representatives of Member States assuming the Presidency of the EU and of data protection authorities such as the EDPS participate as observers.

g) i2010 High Level Group

The EC set up[194] a High Level Group of Member States' representatives to provide advice on the implementation and development of the 'i2010 strategy' policy framework. The EC Decision providing for its creation includes an explicit mention of the EC plan to work ICT issues together with Member

---

[188] It shall be noted that security of processing is inherently linked to the protection of personal data. On security obligations, see Article 17 of Directive 95/46/EC and Article 4 of Directive 2002/58/EC.

[189] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Official Journal, L 77, 13.3.2004, p. 1–11.

[190] Article 8 of Regulation (EC) No 460/2004.

[191] On the convenience of setting up the public-private dialogue without an EC Decision, see: EC (2007), *Commission Staff Working Document Accompanying document to the Communication from The Commission to the European Parliament and the Council on Public-Private Dialogue in Security research and Innovation: Impact Assessment*, SEC(2007) 1138, 11.9.2007, Brussels.

[192] The Forum is to examine projects to which to allocate € 2.135 billion in 2007-13.

[193] Commission Decision of 28 June 2007 setting up the Expert Group on Radio Frequency Identification (2007/467/EC), Official Journal of the European Union, L 176, 6.7.2007, pp. 25-30.

[194] Commission Decision of 15 March 2006 on setting up a high level expert group to advise the European Commission on the implementation and the development of the i2010 strategy (2006/215/EC), Official Journal of the European Union, L 80, 17.3.2006, pp. 74-75.

States, "*notably through the open method of coordination*".[195] The High Level Group is an advisory group falling under the classification of 'experts group'. It is composed of one representative per Member State, and chaired by the EC; additionally, it is open to observers from candidate and EEA countries. The High Level Group is assisted by three thematic sub-groups working on eInclusion, eHealth and eGovernment.

h) Data retention expert group

The 14th recital of Directive 2006/24/EC notes that the EC considers appropriate to establish a group composed of Member Stats' law enforcement authorities, associations of the electronic communications industry, representatives of the EP and data protection authorities, including the EDPS, to discuss the evolution of *"legitimate requirements"* of "*competent authorities"* in the domain. The group was formally established in 2008,[196] but convened already in 2007 and three sessions were held that year.[197] Civil society representatives cannot participate as members, although the EC has the right to invite additional experts (such as representatives of Member States, candidate countries or third countries and of international, inter-governmental and non-governmental organisations) to participate in its meetings as observers.[198]

3.2. Non-institutional Actors

3.2.1. Non-Institutional Networks of Data Protection Authorities

The frontier between the institutional and the non-institutional dimension of the activities of data protection authorities is sometimes difficult to delimit.[199] It could for instance be considered that a body such as the Article 29 Working Party plays the role of a non-institutional actor when its activities transcend its explicitly allocated tasks, for instance when it acts as expanding consultative duties to the third pillar issues. In any case, certain activities in which the data protection authorities engage freely seem to fall under the non-institutional tag, as they do not correlate to any specific mandate imposed on them. Data protection authorities have been traditionally very active in international cooperation, creating a complex range of networks without formal institutional support,[200] through which they have progressively developed a sort of '*community*', sharing common values and a particular agenda. Two networks are especially relevant.[201]

---

[195] *Ibidem,* Recital (1).

[196] Commission Decision of 25 March 2008 setting up the 'Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime' group of experts, (2008/324/EC), Official Journal of the European Union, L 111, 23.4.2008, pp. 11-14.

[197] EDPS (2008), *Annual Report 2007,* Brussels, p. 56.

[198] Article 5(2) of Commission Decision of 25 March 2008 setting up the 'Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime' group of experts, (2008/324/EC).

[199] Some scholars consider that data protection authorities are non-institutional actors even when they are formally established as institutional actors. Heisenberg points out that to decide whether the Article 29 Working Party should be classified as an institution or an interest it needs to be considered that it functionally resembles 'an interest' more than an institution, and therefore opts for the former [HEISENBERG, *op. cit.*, p. 17].

[200] BENNET, Colin J., and Charles D. RAAB (2006), *The Governance of Privacy: Policy Instruments in Global Perspective,* Cambridge, Massachusetts: The MIT Press, p. 95.

[201] They are not the only existing networks of data protection authorities. At Member State level, the existence of a Federal Conference in Germany should also be pointed out; it has celebrated more than 70 meetings and allows the adoption of common strategies. Other international networks exist, as for instance the Red Iberoamericana de Agencias de Protección de Datos, or the Conférence des commissaires à la protection des données de la

a) International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners congregates representatives from the data protection authorities and privacy commissioners from Europe and other parts of the world, including Canada, Latin America, Australia, or New Zealand. The International Conference has already celebrated its 29th meeting. Since 2005, it is calling for the creation of an international convention on data protection and it is organising itself to get to influence governments in this direction.

b) Conference of the European Data Protection Authorities

Representatives of data protection authorities from the Member States of the EU and the Council of Europe meet annually at the Conference of European Data Protection Authorities, which has been lately particularly active on EU third pillar issues. The 2007 Larnaka conference lead to a declaration[202] and common position[203] related to the EU third pillar. The European Conference has moreover set up a Working Party on Police and Justice, mandated to monitor and examine the developments in the area of police and law enforcement, which has been active since 2006[204] and has, among other things, co-published an opinion with the Article 29 Working Party.[205]

3.2.2. The Organised 'Civil Society'

This sub-section explores actors that can fall under the general tag of 'civil society organisations' used by the EC in its policy of consultation.[206] Organisations concerned with data protection law and policy-making at EU level can in principle be classified in two main groups: those advocating a reinforcement or non-erosion of data protection and privacy rights,[207] on the one hand, and those advocating for a limitation of obligations for data controllers and processors, on the other hand. In this section they have been classified into the categories of 'privacy advocacy' and 'other interest parties'.

Francophonie, launched in 2007. An international network of sub-national data protection authorities has also been set up.

[202] European Data Protection Authorities (2007), *Declaration adopted in Cyprus on 11 May 2007*, Cyprus, 11 May.

[203] European Data Protection Authorities (2007), Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement, Cyprus, 11 May.

[204] Commission Nationale de l'Informatique et des Libertés (CNIL) (2007), [*27e Rapport d'activité 2006*, La Documentation Française : Paris, p. 50.

[205] Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data and Working Party On Police And Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007*, WP145, WPPJ 01:07, December.

[206] EC (2002), *Communication from the Commission "Towards a reinforced culture of consultation and dialogue – General principles and minimum standards for consultation of interested parties by the Commission*", COM(2002) 704 final, 11.12.2002, Brussels, p. 6.

[207] This section does not pretend to review all existing organisation and initiatives in the Member States. They are varied and most of them do not pretend to have any direct interaction with EU level decision-making; some focus on concrete aspects related to privacy and data protection and progressively develop a wider interest. As examples can be mentioned the French initiative against RFID for animals [« Des moutons et des hommes »; see: BIAGINI, Cédric and Guillaume CARNINO (2007), *La tyrannie technologique: Critique de la société numérique*, Editions l'Echappée, p. 235]; the Belgian association Collectif de Résistance A la Puce (more information at: http://www.stoppuce.be), or the Dutch Meldpunt Misbruik Identificatieplicht, campaigning against compulsory identification (more information at: http://www.id-nee.nl/).

a) Privacy advocacy

EU civil society organisations are more familiar with the discourse of the right to privacy than with the discourse of the right to the protection of personal data. Generally, concerns related to the protection of personal data are framed in terms of the right to privacy. This does not imply, however, that 'privacy advocacy' as such is vigorous at EU level: on the contrary, there is a general agreement on its relative weakness.[208]

A very limited number of actors dedicated to privacy advocacy are permanently or at least regularly involved in decision-making at EU level. The European organisations explicitly focusing on data protection or closely related rights are only a few, and the majority of them are not particularly present in EU level decision-making. Of the limited number of consistently involved actors, an important part is English-speaking and based in the UK. The UK is also one of the Member States where the public opinion seems more regularly alerted on privacy and data protection issues, sometimes publicised as 'privacy scandals'.[209] Germany can be pointed out as the Member State in which the pro-privacy movement has gained more popularity and visibility, as 'anti-surveillance' demonstrations are regularly being organised since November 2007 by German organisations.[210] The impulse for a pan-European 'anti-surveillance' action to take place in Autumn 2008,[211] certainly the first one of such dimension, came from Germany.[212]

Examples of Pro-Privacy Organisations

This section aims to offer a panorama of existing organisations acting in the defence of the right to privacy, which are the ones that happen to be also involved in supporting data protection. They have been classified in different groups depending on their main focus of activities: anti-surveillance organisations, digital rights advocates, civil liberties advocates, human rights advocates, consumer rights advocates.[213] Important contributions to discussions on data protection are sometimes provided by other entities.[214] A category of organisations whose contribution is generally believed to be

[208] An example given as an illustration of such weakness, especially in contrast with other lobbying forces such as copyright-holders advocates, is the resulting weakness of the EU legislative support for privacy-enhancing technologies, to be compared with the strong legislative support granted for copyright-technologies in Articles 6 and 7 of Directive 2001/29/EC [BYGRAVE, Lee A. (2002), "Privacy-Enhancing Technologies: Caught between a Rock and a Hard Place", *Privacy Law & Policy Reporter*, volume 9, p. 136]. See also: BENNET and RAAB, *op. cit.*, p. 34.

[209] Germany has also experienced recently revelations with a wide impact on public opinion.

[210] For example: 29 December 2007, demonstration "Gegen Vorratsdatenspeicherung, guten Rutsch ins Jahr 1984" in Berlin; 15 March 2008, "Für ein Morgen in Freiheit" demostration in Köln. On 31 May 2008, activities were undertaken simultaneously in more than 30 cities across Germany.

[211] Under the title "Freedom not fear 2008"; more information at: http://wiki.vorratsdatenspeicherung.de/Freedom_Not_Fear_2008.

[212] The action is currently scheduled for 11 October 2008 and is originally an initiative of the German Work Group on Data Retention.

[213] The classification is partially inspired by Colin Bennett's approach, which notably distinguishes: privacy dedicated advocates; Internet rights advocates; consumer advocates; civil liberties advocates; human rights advocates; software provider advocates: information rights advocates; technology specific advocates; academic advocates; activist advocates [BENNET, Colin (2005), *Privacy Advocacy and Activism*: *Spotlighting Surveillance Practices in a Networked World*, talk to "The Concealed" Conference, University of Ottawa, 4-5 March; BENNETT, Colin (2006), *Information Rights and Privacy Advocacy: Online versus Offline activism*, talk to "Information Rights Salon, University of Toronto, 27 March].

[214] For instance, the Dutch Standing Committee Of Experts On International Immigration, Refugee And Criminal Law (Commissie Meijers) takes carefully account of data protection implications of the legislative and policy inititiaves it critically review.

pertinent are trade union associations,[215] even if they cannot be considered to be especially actively involved in privacy advocacy at EU level.

a) Anti-Surveillance Organisations

'Anti-surveillance' organisations focus on the general defence of the right to privacy, which in their view is broadly threatened by the development of 'surveillance' in its different manifestations (the 'surveillance society', the 'surveillance state', 'surveillance technologies', etc). One of the most important organisations of this type is Privacy International (PI),[216] a human rights watchdog focused 'on surveillance by governments and corporations' established in 1990. Privacy International is based in London, even if its activities are, as suggested by its name, international.[217] Another crucial organisation with a strong international dimension is the Electronic Privacy Information Center (EPIC),[218] a 'public interest research center' established in Washington, D.C. and active since 1994. EPIC aims to focus public attention on civil liberties issues and to protect privacy,[219] and works in close cooperation with Privacy International for a series of issues.[220]

Continental 'anti-surveillance organisations' have commonly more limited territorial ambitions. Examples of organisations with a marked national dimension are Souriez Vous Etes Filmés[221], a French association created in 1995 'against surveillance technologies'; the German Non-Governmental Organisation (NGO) STOP1984, mainly concerned with supporting the right on informational self-decision and the protection of privacy[222], and the Austrian ARGE DATEN (Österreichische Gesellschaft für Datenschutz)[223], explicitly focusing on data protection and active since 1983.

b) Digital Rights Advocates

Some 'civil society' organisations have a strong interest in privacy because of their general interest in the defence of information society rights (including, for instance, intellectual property rights). They are usually referred to as 'digital rights advocates'. The European Digital Rights Initiative (EDRi) is a European umbrella organisation created in June 2002 and coordinating the efforts of European and non-European organisations in this field. Currently, 25 organisations possess EDRI membership.[224] An

---

215 POULLET, *op. cit.*, p. 209.

216 More information at: http://www.privacyinternational.org.

217 Privacy International also has an office in Washington, DC.

218 More information at: http://www.epic.org/.

219 EPIC is also responsible for The Public Voice project, which was established in 1996 to promote public participation in decisions concerning the future of the Internet. In cooperation with the OECD, UNESCO, and other international organizations, the Public Voice project brings civil society leaders face to face with government officials for constructive engagement about current policy issues.

220 EPIC notably manages the site Privacy.Org (daily news, information, and initiatives on privacy) together with Privacy International. See: http://www.privacy.org/.

221 More information at: http://souriez.info.

222 More information at: http://stop1984.com.

223 More information at: http://www2.argedaten.at.

224 Current EDRi members are: Association Electronique Libre (AEL) (Belgium); Association for Technology and Internet (APTI) (Romania); ALCEI (Italy); Bits of Freedom (The Netherlands); Campaign for Digital Rights (CDR) (UK); Chaos Computer Club (CCC e.V.) (Germany); CPSR-ES (Spain); Digital Rights (Denmark); Digital Rights (Ireland); Electronic Frontier Finland (EFFI) (Finland); FoeBud e. V. (Germany); Förderverein Informationstechnik und Gesellschaft (FITUG e.V.) (Germany); Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.) (Germany); Foundation for Information Policy Research (FIPR) (UK); GreenNet (UK); Internet Society (Bulgaria); Iuridicum Remedium (Czech Republic); Imaginons un

EDRI member especially active at EU level is the Electronic Frontier Foundation (EFF), founded in 1990, which is based in San Francisco but has an international scope of activities.[225] Examples of other EDRi members are the Austrian Association for Internet Users (VIBE! AT - Verein für Internet-Benutzer Österreichs),[226] the British Open Rights Group (ORG)[227] and the Italian Associazione per la Libertà nella Comunicazione Elettronica Interattiva (ALCEI).[228]

c) Civil Liberties Advocates

Other organisations follow closely EU level data protection and privacy developments in the context of their general monitoring of civil liberties. They are not many. Actually, there is only one organisation routinely playing an important role at EU level, namely Statewatch. Founded in 1991, Statewatch is comprised of lawyers, academics, journalists, researchers and community activists. Its most prominent contributors are based in the United Kingdom (UK). Other actors very often cite Statewatch as a source of otherwise unobtainable information.[229] Statewatch is one of the founding members of the European Civil Liberties Network (ECLN),[230] an umbrella organisation nowadays not very active.

d) Human Rights Advocates

Human rights advocates are also concerned with data protection, at least insofar it affects the (human) right to privacy. At EU level, the relevant umbrella organisation is the European Association for Human Rights (AEDH),[231] which gathers together leagues and associations defending human rights in the EU. It is a partner of the International Federation for Human Rights (FIDH).

e) Consumer Advocates

Both the EC and the Article 29 Working Party have lamented that reaction obtained from consumer protection associations in the different consultations on data protection issues is generally weak.[232] At Member State level, some national consumer associations are expressly concerned with data protection and privacy issues, particularly in their activities related with digital consumer rights, but not

---

Réseau Internet Solidaire (IRIS) (France); Metamorphosis (Macedonia); Netzwerk Neue Medien (NNM e.V.) (Germany); Nodo50.org (Spain); Open Rights Group (UK); quintessenz (Austria); Swiss Internet User Group (SIUG) (Switzerland); VIBE!AT (Austria).

[225] EFF supports for instance the non EDRi member La Quadrature du Net, a French "citizen group informing about legislative projects menacing civil liberties as well as economic and social development in the digital age" (more information at: http://www.laquadrature.net).

[226] More information at: http://www.vibe.at.

[227] More information at: http://www.openrightsgroup.org.

[228] More information at: http://www.alcei.org.

[229] For instance: Réseau UE d'Experts Indépendants Sur Les Droits Fondamentaux (CFR-CDF) (2003), *L'équilibre entre liberté et sécurité dans les réponses de l'Union Européenne et de ses Etats membres à la menace terroriste*, Observation thématique, 31 mars. Statewatch has also been cited as a source by the EDPS [EDPS (2006), *Second opinion on the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, 29 November, Brussels, p. 2].

[230] More information at: http://www.ecln.org.

[231] More information at: http://www.aedh.eu.

[232] POULLET, *op. cit.*, p. 209.

all of them;[233] the economic reliance of certain national consumer associations[234] on marketing campaigns does not contribute to strengthen their involvement in data protection. At EU level, The European Consumer's Organisation (BEUC) plays a leading role.[235] BEUC is moreover a member of the Transatlantic Consumer Dialogue (TACD),[236] a forum of US and EU consumer organisations launched in 1998 and active monitoring fields related to data protection.[237] Another relevant organisation is ANEC, 'the European consumer voice in standardisation', set up in 1995 to defend consumer interests in the process of standardisation and certification, as well as in policy and legislation related to standardisation, and partially funded by the EC.

EU Privacy Advocacy In Action: Two Examples

To complement the overview of EU privacy advocacy, two examples of advocacy 'in action' are described.

a) Mobilization Against The Data Retention Directive

Civil society mobilization against the Data Retention Directive and its implementation provides a particularly interesting example of how can different organisations be involved in the defence of data protection. The mobilization was organised first to influence EU decision-making, in 2005, while the proposal for a Directive on the retention of data generated or processed in connection with electronic and public communications was being drafted and negotiated. Later, as the Directive had been approved and its provisions had to be implemented through national law, mobilization aimed at influencing the different national governments responsible for the implementation. The organisations leading the opposition to the initial proposal at EU level were PI and EDRi. The opposition was structured around a campaign titled "Data Retention is No Solution",[238] consisting mainly in a petition which obtained over 58,000 signatures. When the Data Retention Directive was finally approved, Ireland chose to take the case to the ECJ.[239] The Irish Human Rights Commission introduced an application for permission to intervene in the case as amicus curiae. In Germany, the campaign against the implementation of data retention was organised via an ad-hoc working group, the Arbeitskreis Vorratsdatenspeicherung (German Working Group on Data Retention)[240], an association of civil rights campaigners, data protection activists and Internet users, which also launched the

---

[233] An illustration of the minor involvement of consumer advocates in privacy and data protection issues can be found in a report commissioned by ANEC on RFID, in which it is stated that "[*g*]*iven the nature and scale of RFID deployment now in operation, surprisingly few of the organisations contacted have developed any kind of policy response*" [MEEK, Colin (2008), *Consumer requirements for RFID standardisation,* Intertek Research and Performance Testing Report, commissioned by the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC), p. 8]. Interestingly, two of the national organisations contacted mention as relevant activities the participation in an EC workshop on RFID.

[234] For instance, the Belgian Test-Achats (http://www.test-achats.be/).

[235] More information at: http://www.beuc.eu.

[236] More information at: http://www.tacd.org.

[237] For instance, in its report summarizing the 2006 recommendations to the EU, it addresses the following subjects: Passenger Name Records; Identity Theft, Phishing and Consumer Confidence; Internet Security; Digital Rights Management [TRANSATLANTIC CONSUMER DIALOGUE (TACD) (2007), *2006 Recommendations report and European Commission Services' Responses*, May].

[238] More information at: http://www.stopdataretention.com.

[239] Action started on 6 July 2006, *Ireland vs. Council of the European Union, European Parliament* (Case C-301/06). Digital Rights Ireland started litigation in September 2006 in Ireland challenging the Directive and Ireland's domestic laws, alleging that the provisions are procedurally flawed and are also in breach of the right to privacy guaranteed under the Irish Constitution and Article 8 ECHR.

[240] More information at: http://www.vorratsdatenspeicherung.de.

initiative of introducing to the ECJ an 'amicus curiae' brief signed by 42 different organisations.[241] In Denmark, opposition was lead by the IT-Political Association of Denmark. In Belgium, a petition against data retention provisions has been launched by the human rights association Liga voor Mensenrechten. In Hungary, the Hungarian Civil Liberties Union (HCLU)[242] filed a complaint with the Hungarian Constitutional Court in May 2008, requesting the examination and annulment of Hungarian data retention provisions implementing Directive 2006/24/EC.

b) The Google/DoubleClick merger

The Google/Doubleclick case can be mentioned as an illustration of privacy advocacy operating with far less visibility and almost no direct involvement of the population. The case concerns the decision that had to be taken by the EC on a merger of the companies Google and DoubleClick. The EC had no legal obligation to take into account data protection or privacy implications of the merger before adopting a decision. Nevertheless, there was some concern on such implications amongst 'civil society' representatives and data protection authorities. BEUC sent at letter to the EC asking for a check on the privacy aspects of the deal. PI sent also a letter to the responsible Commissioner expressing similar concerns.[243] EDRi expressed public support for the letter. The Data Protection Commissioner of the German state of Shleswig-Holstein publicly opposed the Google's acquisition of Doubleclick in another letter to EU Competition Commissioner.[244] The EC eventually cleared the acquisition.

b) Other Interested Parties

Other parties 'interested' in EU law and policy-making related to the right to data protection can potentially be all data controllers and processors. Some economic fields, however, are especially dependent on the processing of personal data and feel particularly concerned. The Federation of European Direct and Interactive Marketing (FEDMA) has traditionally been a very active player.[245] The Interactive Advertising Bureau Europe (IAB Europe), the pan-European trade association of digital and interactive marketing representing national associations, is also following developments very closely. Other interested parties include the Business Software Alliance (BSA), the European Software Association, and actors related to the management intellectual property rights, or digital rights management (for instance, the Digital Watermarking Alliance).[246] Lobbying initiatives are traditionally triggered by discussions on legislatives proposals. The negotiations leading to the adoption of the Data Protection Directive were a crucial moment for the organisation of the sector.[247]

---

[241] The brief was introduced in April 2008. For the list of signatories: http://www.vorratsdatenspeicherung.de/content/view/216/79/lang,en/#Signatories.

[242] More information at: http://www.tasz.hu.

[243] On 5 November 2007.

[244] These lobbying initiatives had no particular impact on the final decision.

[245] Major reorganization and 'activation' of representatives in the filed took place during the negotiations leading to the Data Protection Directive [BENNET and RAAB, *op. cit.*, p. 95].

[246] More information: http://www.digitalwatermarkingalliance.org. The Digital Watermarking Alliance includes a Digital Watermarking Working Group author for instance of a document in which "*11 of the world's leading providers of digital watermarking*" address what they perceive to be the inappropriate association of digital watermarking technology with privacy concerns [Digital Watermarking Working Group (2005), Digital Watermarking Working Group's Response to Privacy Concerns Raised by Paper WP 104 from the European Union's Data Protection Working Party (Response to EU Paper WP 104), Digital Watermarking Alliance, 31 March, p. 1].

[247] On the lobbying pressure from US companies, see: REGAN, Priscilla M., "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics" in BENNET, Colin J. and Rebecca

3.2.3. The (Uninterested?) Data Subject

The fundamental right to data protection is a right granted to 'everyone'.[248] In EU legal instruments, and notably in the Data Protection Directive, the natural person enjoying the right to the protection of his or her personal data ('everyone') is conceptualised as the 'data subject'.[249] The right to the protection of personal data is based on the assumption that 'the data subject' is an autonomous, potentially active subject, to be entrusted with a series of rights to balance the unbalanced division of powers between him or her and the 'data controllers' (legally responsible for the processing). In order to refine this vision of 'the data subject' as an actor directly involved in law and policy-making, two different aspects can be examined: (a) the possible negotiation of the protection of personal data granted by the law in daily expressions of consent to disclosure or to the processing of personal data;[250] (b) the integration in decision-making of the concerns of 'the data subject' as expressed directly (and not through representation modes).

(a) EU data protection legislation places in the hands of the 'data subject' the possibility to *freely consent* to certain data processing practices.[251] Individuals envisioned as empowered 'data subjects' could be considered as theoretically able to re-present directly their own data protection preferences through 'consent', in almost constant negotiations with data controllers and processors. As a matter of fact, however, the modalities of the consent to the processing can transform it into a mere formality, replacing the data subject in an inferior, vulnerable position. Consent as a ground for legitimate processing has been strongly criticised,[252] and should in any case not be used as a trustable indicator of the population preferences or concerns (or lack of) regarding data protection.

(b) The most 'direct' method used by the EC to monitor the population's views on data protection law is the use of surveys.[253] In 2003, two '*Eurobarometer*' opinion surveys were conducted for the EC.[254] One looked at EU citizen's views on privacy relating to information held about them by a variety of public and private organizations, as well as related data protection issues, via face-to-face interviews. The other collected EU companies' views about privacy via telephone interviews. Two other similar surveys were conducted in January 2008,[255] upon the request of DG Justice, Freedom and Security. According to the results, a majority of EU citizens show concern about data protection issues: 64% of respondents said that they were concerned as to whether organisations that held their personal data

---

GRANT (eds.) (1999), *Visions of privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, pp. 199-216.

[248] Article 8(1) of the EU Charter of Fundamental Rights: "1. Everyone has the right to the protection of personal data concerning him or her."

[249] Article 2(a) of Directive 95/46/EC.

[250] Article 8(2) of the EU Charter of Fundamental Rights: "... *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*".

[251] Article 2(h) of Directive 95/46/EC: "(h) "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

[252] See, for instance: POULLET, Yves and Jean-Marc DINANT (2004), L'autodétermination informationnelle à l'ère d'Internet: Eléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif (T-PD), Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, Strasbourg, 18 novembre, p. 42.

[253] Another method of presumably direct contact with the data subjects concerns is through the 'openness' of 'open consultations', even if the representative dimension of the 'interested citizens' directly participating in them cannot be considered satisfactory.

[254] They were reviewed by the EC in its 2003 report on the implementation of Directive 95/46/EC.

[255] Gallup Organization (2008), *Data Protection in the European Union: Citizens' perceptions*, Analytical Report, Flash Eurobarometer 225, February.

handled the data appropriately.[256] At the same time, a majority of EU citizens appear to feel that their fellow citizens have low levels of awareness about data protection: 77% of respondents said that people's awareness in their own country was low.[257]

4. CURRENT PRACTICES

This section reviews current practices regarding the design of data protection law and policy in the EU, as well as with respect to the integration of data protection concerns in EU law and policy-making in general. The practices examined concern aspects of decision-making such as the integration of the citizen and of non-institutional actors into the decision-making process (for instance, through consultation procedures); they also include the screening of law and policy proposals compliance with fundamental rights, and evaluation procedures that potentially promote the transfer on learning amongst actors. Practices in the context of research funding and regarding international cooperation have also deserved special attention.

4.1. Consultations

One of the main techniques used by EU institutions to integrate in law and policy-making the concerns of other actors are consultations, which allow them to 'directly' interact with interest groups.[258] The EC is the EU institution organising consultations more regularly; it can decide to held consultations at any moment during the legislative process.[259] The EC officially opens consultations to all 'interested parties', a wide notion actually comprising all those who wish to participate in consultations run by the EC. Data protection can be the main subject of a consultation procedure, or pop up indirectly in consultations on other subjects.[260] Studies are sometimes launched in the context of consultations, to serve as a reference point for the debate.[261]

---

[256] The figures range from 86% in Germany and Austria to 32% in The Netherlands, 34% in Bulgaria and 36% in Finland [Gallup Organization (2008), *Data Protection in the European Union: Citizens' perceptions*, *Analytical Report*, Flash Eurobarometer 225, February, p. 7].

[257] The figures range from 93% in Greece and 90% in Cyprus and Hungary to 56% in Luxembourg and 59% in Denmark [Gallup Organization (2008), *Data Protection in the European Union: Citizens' perceptions*, *Analytical Report*, Flash Eurobarometer 225, February, p. 20].

[258] EC (2002), Communication from the Commission "Towards a reinforced culture of consultation and dialogue – General principles and minimum standards for consultation of interested parties by the Commission", COM(2002) 704 final, 11.12.2002, Brussels, p. 4.

[259] EC (2002), Communication from the Commission "Towards a reinforced culture of consultation and dialogue – General principles and minimum standards for consultation of interested parties by the Commission", COM(2002) 704 final, 11.12.2002, Brussels, p. 4.

[260] Privacy and data protection are "ethical issues" identified as relevant for a discussion on Ageing well in the Information Society in an EC Action Plan on the issue. They were addressed for instance in a workshop celebrated on 29 October 2007, organised by DG INFSO, Unit: ICT Addressing Societal Challenges, ICT for inclusion, considered as a first step in initiating a deeper discussion on ethics and e-inclusion and is to be followed by a second one in May 2008 and a high-level panel discussion as a part of i2010 Conference under Slovenian Presidency.

[261] This was the case in the context of the consultation on the protection of worker's personal data. See: HENDRICKX, Frank (2002), *Protection of worker's personal data in the European Union: Two studies: 1. Study on the protection of workers' personal data in the European Union: general issues and sensitive data; 2. Study on the protection of workers' personal data in the European Union: surveillance and monitoring work*, July.
Two studies were prepared for the EC with the aim to provide a comprehensive picture of the relevant regulatory framework in the EU Member States:
- Contract study VC/2002/0102, for a study on the protection of workers' personal data: general issues and sensitive data. Contractor: Frank Hendrickx. Research undertaken with a group of experts specialised in the field of data protection and employment privacy. Study concluded in 2002.

The origins of consultation procedures as an established EC practice can be linked to social dialogue, which has itself been relevant for the examination of data protection in the employment sector.[262] In 2000, indeed, the EC included in the European Social Agenda[263] an action concerning the protection of workers' personal data in the workplace.[264] Subsequently, it consulted the social partners[265] on the advisability (at a first stage) and the content (a at a second stage) of a Community initiative in the area.[266] Despite the divergent positions observed during the first phase,[267] the EC had considered advisable to establish employment sector specific rules at Community level. However, no public statement or related initiative followed up the second phase of the consultation.[268]

Since then, the EC has developed specific consultation practices not limited to social dialogue. Consultation procedures are currently quite numerous, even if variable in dimension and in nature; actually, there remain questions about how systematic the process of consultation is.[269] Consultations only exceptionally concern third pillar issues.

Officially, the EC practice of performing consultations simply coexists with the activities of existing consultative bodies such as the already mentioned ESC or the Committee of the Regions,[270] which coexist also with regular formal and informal exchanges with experts and Member States representatives,[271] as well as with the specific consultative tasks of special consultative bodies such as the relevant 'expert groups' active in the area. The two main specific consultative bodies on data protection, namely the Article 29 Working Party and the EDPS, tend to play a variable role during

---

- Study on the protection of workers' personal data in the EU: surveillance and monitoring at work. Contractor: Frank Hendrickx. Research undertaken with a group of experts specialised in the field of data protection and employment privacy. Study concluded in 2001.

The studies were commissioned by the EC following a specific request of the social partners [EC (2002), *Second stage consultation of social partners on the protection of workers' personal data*, 31 October].

[262] EC (2001), Communication from the Commission: First stage consultation of social partners on the protection of worker's personal data (retrieved from: http://ec.europa.eu/employment_social/labour_law/documentation_en.htm).

[263] Endorsed by the European Council at the Nice Summit in December 2000.

[264] One of the main objectives outlined in the Social Policy Agenda of the EC (COM2000/379final, 28.6.2000) was to ensure the development and respect of fundamental social rights as a key component of an equitable society and of respect of human dignity, including the protection of personal data of individuals in the employment relationship. The European Commission had first addressed the issue in a 1997 Communication, *The Social and Labour Market Dimension of the Information Society: People First – Next Steps*, where the Commission committed itself to the adoption of a Communication on data protection in the employment area. Experts from the Member States were invited to several meetings at the time.

[265] On the basis of Article 138 of the Treaty of Rome.

[266] Prior to the launching of the consultation, the EC had requested the Article 29 Working Party to issue an opinion on the application of Directive 95/46/EC to the protection of workers' personal data.

[267] There was a clear divergence between the responses of the employers' organisations, on one side, and the workers' organisations, on the other. The employers' organisations did not see any need for Community legislation on the subject. On the other side, all employees' organisations were in favour of a Community directive on the matter.

[268] DE SCHUTTER, Olivier (2005), "Article II-68 – Protection des données à caractère personnel", in L. Burgorgue-Larsen, A. Levade, F. Picod (eds.), *Traité établissant une Constitution pour l'Europe. Commentaire article par article*, Bruxelles: Bruylant, p. 147.

[269] TONER, Helen (2006), "Impact assessments and fundamental rights protection in EU law", *European Law Review*, 31, June, p. 317.

[270] Prior to the launching of the consultation, the EC had requested the Article 29 Working Party to issue an opinion on the application of Directive 95/46/EC to the protection of workers' personal data, p. 4.

[271] For instance, even if the EC has a consultative body on ICT to discuss the i2010 strategy, it can decide to first consult Member State representatives using a questionnaire and only in a second step to validate the results in the 'expert group' [EC (2008), *Agenda for the 7th meeting of the i2010 High Level Group,* 27 June, Brussels, p. 3].

consultation procedures. In practice, they are sometimes involved as representing 'an interested party', while in certain occasions they organise or co-organise the consultation,[272] in other cases they seem to enjoy the position of a 'privileged interested party' and contribute to consultations issuing formal opinions. Sometimes, finally, they might not be involved in the consultations at all: in this sense, for instance, the EDPS has found regrettable that neither its body nor any other representatives from data protection authorities were consulted during the preparation of communications related to measures entailing large processing operations of personal data.[273]

4.1.1. Examples of consultations in the context of scheduled reviews

Major EU legal texts generally foresee amongst their provisions a regular review and eventual update (on this subject, see also Section 4.4.1). Consultations can take place in the context of such reviews.

- Review of the Data Protection Directive

The EC launched a consultation procedure on the Data Protection Directive in the summer of 2002, to culminate in a report to the EP on the possible revision of the Directive. The review process was mandated under Article 33 of the Data Protection Directive.[274] As part of said review, the EC attempted to give parties other than governments and data protection authorities an opportunity to communicate their opinions. To this end, the EC (1) issued online questionnaires, (2) requested 'position papers' and (3) arranged a conference.[275] (1) The questionnaires were put online in June 2002, with the response deadline of 15 September 2002. Illustrating the non-representative nature of the 'survey', it can be mentioned that 40% of the respondents encoded Germany as their place of residence. (2) The deadline given for 'position papers' was the end of August 2002; most of the papers received came from business groups. (3) The conference was held in Brussels on 30 September and 1 October 2002.

- Review of electronic communications framework

[272] The Article 29 Working Party happens to cooperate sometimes in organising consultations with the EC. It has also sometimes consulted on its own non-institutional actors, and for instance it sometimes organises open workshops (it celebrated a "Workshop on EU approach towards a new passenger data agreement" on 26 March 2007 in Brussels, with the participation of representatives of the EC, the EP, national administrations, national parliaments, academicians, the civil society and the industry). Identification of the actors consulted by the Article 29 Working Party is however generally not detailed: for instance, it stated that it consulted "*the industry*" to prepare WP100 [Article 29 Working Party (2005), *Eight Annual report of the Article Working Party on Data Protection (covering the year 2004)*, adopted in November, European Communities, p. 6].

[273] EDPS (2008), Preliminary Comments on Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union" COM(2008) 69 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final, 3 March, Brussels, p. 2.

[274] Requires regular reporting on its implementation and, if necessary, pertinent amendments.

[275] For more details, see: BYGRAVE, Lee A. (2002), "The 1995 EC Directive on data protection under official review – feedback so far", *Privacy Law & Policy Reporter*, volume 9, pp. 126-129.

A consultation was held in the context of the review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC.[276] The consultation included two phases. Phase I was a 'call for input' that started at the end of 2005 and resulted in around 160 written submissions. The views submitted were used for the preparation of an EC Communication published in June 2006, an accompanying Staff Working document and an Impact Assessment. Based on these documents, the Phase II of the consultation was launched. It ran until October 2006 and it included a public workshop.[277] The Article 29 Working Party published an ad-hoc opinion.

4.1.2. Examples of consultations on specific subjects

Consultations can also be launched on different topics, sometimes following or preceding the publication of a Green Paper or, now more generally, an EC Communication.

- Traffic Data Retention

This consultation was launched jointly by DG Information Society and DG Justice and Home Affairs in 2004. The intention was to identify and discuss data retention practices for both business and law enforcement purposes in the Member States, but also explicitly to address the extent of the need for, and the possible characteristics of, an EU-wide regime of data retention for law enforcement purposes. The consultation was launched after four Member States tabled a proposal for a Council Framework Decision on Data Retention under Title VI of the Treaty on EU. More particularly, it was launched partly as a reaction to demands for open and transparent debate voiced out by the EP and the industry.[278] During the consultation, the EC issued a document and welcomed contributions on it.[279] A public workshop was also celebrated. Contributions were requested from *"all interested parties, including Member States, law enforcement authorities, data protection authorities, industry and consumers/citizens*".[280]

- Detection Technologies

The consultation, celebrated in 2005 and 2006, took the form of a conference[281] and the publication of a Green Paper.[282] The Article 29 Working Party was explicitly invited to participate in the procedure

[276] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal of the European Communities, L 108, 24.4.2002, p. 33-50.
[277] EC (2007), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and Summary of the 2007 Reform Proposals, COM(2007)696 rev1, p. 5.
[278] The DG INFSO / DG JAI consultation document explicitly references "EP Recommendation for second reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, A5-0130/2002, 22 April 2002" and "the EP report of 24 February 2004 on the First Report on the implementation of the Data Protection Directive (95/46/EC), A5 0104 -2004".
[279] EC (2004), DG INFSO – DG JAI Consultation document on Traffic Data Retention, 30 July, Brussels, p. 1.
[280] *Ibidem*, p. 3.
[281] Titled Public-Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against terrorism, held in Brussels on 28-29 November 2005.

and contributed by issuing an opinion.[283] However, in the its opinion the Working Party lamented the vague terms of the Green Paper, which allegedly rendered difficult the provision of a legal analysis of the subject from the point of view of privacy and data protection.[284]

- Location Based Services

This consultation was organised by DG Information Society and Media. It aimed to investigate practices and legal challenges for the offer and use of location-based services. The Article 29 Working Party participated by publishing a specific document on the subject.[285] This consultation was based on publication of 'an issue paper'[286] and the invitation to provide contributions at a workshop[287] or by email.

- Implementation of the Spam Communication

A consultation was launched on the implementation of the EC Communication on unsolicited commercial communications or 'spam'.[288] It was organised by DG INFSO and the Dutch presidency and took the form of questionnaires and an open workshop.[289] The EC intended to assess the effectiveness of the actions undertaken, and to determine whether additional or corrective action was needed. A publicly available questionnaire was addressed to the industry, while another questionnaire was circulated to Member States and competent authorities.[290] The consultation referred mainly to the monitoring of recommended self-regulatory practices and could also be interpreted as an evaluation practice.

- Radio Frequency Identification Devices (RFID)

---

[282] EC (2006), Green Paper on detection technologies in the work of law enforcement, customs and other security authorities, COM(2006) 474 final, 1.9.2006, Brussels, p. 4.
[283] Article 29 Working Party (2007), Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities, WP129, 00039/07/EN, 9 January.
[284] *Ibidem*, p. 7.
[285] Article 29 Working Party (2005), Opinion on the use of location data with a view to providing value-added services, WP 115, November, 2130/05/EN.
[286] EC (2005), Location-based services and the e-Privacy Directive 2002/58/EC: An issue paper for the EU Workshop to be held in Brussels on 12 July 2005, DG Information Society and Media Working Document, 14 June, Brussels.
[287] "Location-Based Services: privacy challenges" Open Workshop, 12 July 2005, Brussels. Were consulted: representatives of the industry, data protection authorities and consumer associations.
[288] EC (2004), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited communications or 'spam'*, COM(2004) 28 final, 22.01.2004, Brussels.
[289] Celebrated on 15 November 2004.
[290] EC (2004), Questionnaire on the implementation of the Communication on unsolicited commercial communications or 'spam' (COM (2004) 28), 'the Communication'), October, Brussels, p. 1.

An online public consultation on RFID[291] was held from July to September 2006.[292] The questionnaire was based on the results of a series of workshops organised in the first half of 2006. In total, 2.190 respondents answered, including citizens, manufacturers, system integrators, academic and scientific institutions, public bodies and regulators. About 70% of all answers were from 'interested citizens', and only 8% of the respondents were female. The headline issue for most of respondents was privacy. A public conference on the results of the online consultation was held on 16 October 2006. In March 2007, the EC held an RFID forum in Brussels and released a communication on steps toward a policy framework, outlining some ideas and asking for comments. In July 2007, European consumer groups ANEC and BEUC issued a joint policy paper in response. The groups suggested that a European committee dealing with ethics should be created and consulted concerning any RFID or near field communication (NFC) technology applications.[293]

4.1.3 Examples of less formalized consultations

Consultation activities can take place outside the structured path of an official consultation procedure.[294] While consultations in the first pillar tend to be formalized, they generally remain informal in the third pillar. As an example can be mentioned the publicly announced intention of the Vice-President responsible for Justice, Freedom and Security to initiate a consultation "*involving the Ministries responsible for law enforcement cooperation as well as the Data Protection Authorities"* in the context of the EC duty to present proposals in 2005 taking into account the Tampere objectives: the consultation seems to have consisted in practice in inviting the EDPS to a meeting, and representatives of other data protection authorities to another meeting.[295] Another example can be found in the context of the preparation of a legislative proposal to provide Member States' police and other law enforcement authorities with access to Eurodac:[296] in the view of preparing the ad-hoc Impact Assessment, the EC convened during autumn 2007 three separate meetings and 'relevant stakeholders' identified by EC services were invited.[297]

The EC has claimed that "*extensive consultations*" took place during the preparation of the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. The consultation procedure seems to have comprised a series of contacts with representatives of Member States, the national data protection authorities of the Member States, the

[291] Originally in English and later translated from English into French, German, Spanish, Italian, Dutch and Polish. More information: http://www.rfidconsultation.eu.

[292] EC (2007), Results of the public online consultation on future Radio Frequency Identification Technology Policy "The RFID Revolution: Your voice on the challenges, opportunities and threats" accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, COM(2007)zzz final, SEC(2007)312, Brussels.

[293] Electronic Privacy Information Centre (EPIC), Privacy & human rights 2006: an international survey of Privacy laws and Developments, EPIC and Privacy International, p. 150.

[294] The Council has its own practices of collection of information, notably through the sending of questionnaires, which are examined in the section on evaluation practices. The non-open nature of this information gathering renders inappropriate its categorization in the same group with EC consultation procedures.

[295] FRATTINI, Franco (2004), *Data protection in the area of Justice, Freedom and Security*, Speech for Meeting with the Joint Supervisory Authorities under the Third Pillar, SPEECH/04/549, Brussels, 21 December, p. 5.

[296] The legislative process to prepare a proposal based on Title VI of the Treaty of the European Union in conjunction with a proposal based on Title IIV of the Treat establishing the EC, amending Eurodac Regulation, followed the conclusions of the JHA Council of 12-13 June 2007.

[297] Relevant stakeholders were identified as: representatives of the law enforcement authorities (25-26 September 2007), representatives of civil society (8 October 2007), and representatives of data protection authorities and the EDPS (11 October 2007). Representatives of the 'civil society' included representatives from the Dutch Commissie Meijers and Amnesty International [Standing Committee Of Experts On International Immigration, Refugee And Criminal Law (Commissie Meijers) (2007), *Note to Mr. Jacques Verraes on the proposal to give law enforcement authorities access to Eurodac*, 6 November, p. 5].

EDPS, the Air Transport Association of America, the International Air Carrier Association and the International Air Transport Association.[298] Several meetings with them were organised, contacts took place, and a questionnaire was sent out.[299] The lack of participation of 'civil society' representatives in this procedure can be noted.

4.2. Impact Assessments

Believed to support openness and 'better regulation',[300] impact assessments constitute an important part of the EC legislative drafting and policy preparation process since 2002. Since 2005, all legislative and major policy defining proposals contained in the EC legislative and work programme must be subject to an impact assessment. Additionally, some actors have explicitly called for an extension of the EC obligations to the legislative proposals supported by Member States (in the third pillar).[301]

'Integrated' impact assessments can be performed during consultation procedures, even if it is more common for consultation procedures to be organised in the context of the preparation of an impact assessment. Impact assessments should normally be conducted in two separate phases: a preliminary stage determining the eventual need for a full, extended impact assessment, and a second stage including consultation with interested parties and relevant experts, to be conducted following the general guidelines on consultations.[302] According to the general EC guidelines for impact assessments, the consultation for an impact assessment shall start with a 'consultation plan' identifying the objective of the consultation; the elements of the impact assessment for which consultation is necessary; the target group; the appropriate consultation tool(s) and the appropriate time for consultation(s).[303] In 2006, the EC established an independent Impact Assessment Board to monitor and eventually improve the consistency and quality of EC impact assessments.

4.2.1. Impact Assessments and Data Protection

The link between 'integrated' impact assessments and fundamental rights protection represented a major element of the EC strategy for fundamental rights protection during the legislative process published in April 2005.[304] Impact assessments relate to fundamental rights inasmuch as they include

[298] EC (2007), Accompanying document to the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Summary of the Impact Assessment, Commission Staff Working Document, SEC(2007) 1422. Brussels, p. 2.

[299] EC (2007), Proposal for a Council Framework Decision on the Use of a Passenger Name Record (PNR) for law enforcement purposes, presented on 6 November, p. 4.

[300] On impact assessments as an element of the EC action plan on better law-making, see: ALLIO, Lorenzo (2007), "Better regulation and impact assessment in the European Commission", in KIRKPATRICK, Colin and David PARKER, *Regulatory Impact Assessment: Towards better regulation?*, Edward Elgar, pp. 72-105.

[301] House Of Lords European Committee (2007), *Prüm: an effective weapon against terrorism and crime?*, Report with Evidence, HL Paper 90, 18th Report of Session 2006-07, The Stationary Office Limited: London, 9 May, p. 23.

[302] TONER, *op. cit.*, p. 321.

[303] EC (2005), *Impact assessment guidelines*, SEC(2005) 791, 15 June, Brussels, p. 9. Minimum standards for consultation in the process and reporting shall be respected, in accordance with COM(2002)704, paying particular attention to transparency (*ibidem*, p. 11). Consultation may be open to the general public, restricted to a specific category of stakeholders (any member in the selected category can participate) or limited to a set of designated individuals/organisations (only those listed by their names can participate). You should always include all target groups and sectors that will be significantly affected by or involved in policy implementation, including those outside the EU (ibidem, p. 10).

[304] TONER, *op. cit.*, p. 316. The EC distinguished between the roles in this strategy for impact assessments (which should include as full and precise a picture as possible of the different impacts on individual rights) and

the review of the potential impact of the assessed proposal on such rights, including explicitly the right to privacy and the right to the protection of personal data. In the template for impact assessments, private life and personal data are mentioned in a table summarizing the 'social impacts' to be reflected upon.[305] The decision not to create a separate category for the review of the 'impacts on fundamental rights', but rather to integrate these impacts into the three existing categories (economic, social and environmental impacts) was a deliberate choice of the EC.[306] The link between impact assessments and fundamental rights is further reinforced by the obligation for the EC, when conducting consultations with concerned parties, the 'civil society' and 'the general public' in order to prepare an impact assessment, "*to draw attention to the rights set out in the Charter and its own internal monitoring of respect for those rights by inviting the parties consulted to assert their fundamental rights".*[307]

When the Data Protection Directive was drafted and discussed, impact assessments were not yet an established practice at EU level, even if the practice of conducting assessments of the *economic* impact of proposals was already established in certain Member States. During the discussions leading to the adoption of the Data Protection Directive it appeared that some national administrations managed certain studies assessing the financial impact of the proposal.[308] Eventually, as the potential costs of implementation became increasingly central to the debate, the EC appointed independent researchers to undertake a detailed cost-benefit analysis of the proposed directive in the UK and in the Netherlands.[309]

Representatives from the data protection authorities are generally very keen to prone the wide necessity of impact assessments. In this sense, the EDPS underlined in his opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability that in so far the proposal laid down exchanges of DNA data, it could be adopted only after the publication of an impact assessment.[310] The EDPS also called on the Council to include an impact assessment in the procedure leading to the integration of the Prüm Treaty at EU level.[311] The Europol

---

explanatory memoranda (dealing essentially with the legal basis for compliance with fundamental rights) [MEUWESE, Anne (2008), *Impact assessment in EU law making*, E.M. Meijers, p. 91].

[305] Key questions highlighted on the issue are: "Does the option affect the privacy of individuals (including their home and communications) or their right to move freely within the EU? Does it affect family life or the legal, economic or social protection of the family? Does the option involve the processing of personal data or the concerned individual's right of access to personal data?", EC (2005), Impact assessment guidelines, SEC(2005) 791, 15 June, Brussels, p. 32.

[306] MEUWESE, *op. cit.*, p. 92; see also: EC (2005), Communication from the Commission: Compliance with the Charter of Fundamental Rights in Commission legislative proposals: Methodology for systematic and rigorous monitoring, COM(2005) 172 final, 27.4.2005, Brussels, p. 5.

[307] EC (2005), *Communication from the Commission: Compliance with the Charter of Fundamental Rights in Commission legislative proposals: Methodology for systematic and rigorous monitoring*, COM(2005) 172 final, 27.4.2005, Brussels, p. 8.

[308] The UK government relied on studies undertaken by the UK Home Office and the UK Department of Health to declare that the approval of the proposal would result in disproportionate costs, while the House of Lords called for an assessment to be provided for the Council prior to the final decision. The Dutch Ministry of Economic Affairs eventually decided to undertake a survey of private sector organisations [see: PEARCE and PLATTEN, *op. cit.*, pp. 534-35].

[309] *Ibidem*, p. 537.

[310] EDPS (2006), Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final), Official Journal C 116, 17.5.2006, p. 17.

[311] EDPS (2007), Opinion on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with the

Joint Supervisory Body has underlined that any moves in the direction to make EU-wide information systems with related purposes interoperable ought to be preceded by a Privacy-Impact Assessment (PIA), assessing the potential implications for the rights of individuals.[312]

Even if the right to privacy and the right to data protection are to be considered in the context of the preparation of EC impact assessments, these assessments are in many ways different from PIAs, in which the impact on privacy and data protection is a central issue. Moreover, while impact assessments may be used to examine and scrutinise proposed legislation and policy,[313] privacy impact assessments are more project-oriented and appear to be more convenient for the design and implementation of specific systems.[314] The EDPS has expressed its support for the obligation to carry on exhaustive privacy impact assessments before new EU systems processing personal data are developed.[315]

4.2.2. Examples of Impact Assessments

The present sub-section provides a series of examples illustrating the use of impact assessments and some of its limitations.[316]

- Visa Information System (VIS)

An assessment of "*the impact on privacy and human rights*" of the VIS was included in the pertinent extended impact assessment published in 2004, together with the proposal for a VIS Regulation.[317] In order to compare the costs of the alternative policy options with regard to the establishment of VIS, the extended impact assessment described the "*impact on privacy and human rights*" alongside "*financial costs*", "*opportunity costs"* and "*reductions in business travel and tourism*". Both with regard to the policy option of establishing an entry/exit system based on VIS and the establishment of VIS including biometrics, the impact assessment study emphasised their extensive impact on the protection of the

---

view of adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime, 4 April, Brussels, p. 16.

[312] Europol Joint Supervisory Body (2005), The Second Activity Report of the Europol Joint Supervisory Body: November 2002 – October 2004, p. 26.

[313] TONER, *op. cit.*, p. 317.

[314] Supporting a more widespread use of PIAs, see also MURAKAMI WOOD, David and Kirstie BALL (eds.) (2006), *A Report on the Surveillance Society, for the Information Commissioner by the Surveillance Studies Network,* September, pp. 89-90.

[315] EDPS (2008), *Preliminary Comments on Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union" COM(2008) 69 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Examining the creation of a European Border Surveillance System (EUROSUR), COM(2008) 68 final, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final*, 3 March, Brussels.

[316] Many other examples could be mentioned, such as the impact assessment performed in the context of the review of the e-Privacy Directive, which was introduced in the context of a series of three legislative proposals accompanied by an impact assessment and a communication setting out the main policy lines and reporting on the prior public consultation [EC (2007), *Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, COM(2007) 698 final, 13.11.2007, Brussels, p. 2].

[317] EC (2004), Commission Staff Working Document Annex to the Proposal for a Regulation to the European Parliament and to the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas: Extended Impact Assessment, SEC(2004) 1628, 28.12.2004, Brussels.

right to privacy. The impact assessment was performed with the help of an external contractor, responsible for *"providing general advice or studying specific points (e.g. data protection and the use of biometrics*)"[318]. The EC, when publishing the proposal on the VIS Regulation, simply stressed that it respects the fundamental rights and observes the principles recognised in particular by the EU Charter of Fundamental Rights. In the explanatory memorandum, the EC did not mention the right to privacy.[319]

- Council Framework Decision on third pillar data protection

In this impact assessment[320] the EC considered six different options in order to provide for an appropriate legal regime for data processing and protection in the course of police and judicial cooperation in criminal matters. It assessed the impact of the options on public security, fundamental rights, in particular the right to data protection, on the consistency of EU data protection policy and on costs. To prepare the impact assessment, a series of procedural steps and consultations were undertaken.[321] The main purpose of the consultations was to find out whether a legal instrument on the processing and protection of personal data in the third pillar was needed and, if so, what should be the main content of such an instrument. Consultations took place based on a questionnaire and a discussion paper.

- Data Retention

This impact assessment was undertaken in the context of competence disputes between the Council, on the one hand, and the EC and the EP, on the other.[322] The proposal assessed regarded the retention of personal data, and did not figure in the relevant EC legislative and work programme. However, there was strong political pressure for an impact assessment to be performed and it was prepared, in only two weeks,[323] using as input the information obtained previously through two meetings organised on the issue (one with national experts from justice departments, and a second

[318] Ibidem, p. 4.
[319] BROUWER, Evelien (2006), Digital Borders and Real Rights: Effective remedies for third-country nationals in the Schengen Information System, Centre for Migration Law, Radbourd University Nijmegen: Nijmegen, p. 130.
[320] EC (2005), Impact Assessment Annex to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, Commission Staff Working Document, COM(2005) 475 final, 4.10.2005, Brussels.
[321] On 22 November 2004 and on 21 June 2005, the EC invited and consulted experts representing the governments of the Member States, Iceland, Norway and Switzerland. On 11 January 2005, it convened a consultative meeting with the data protection authorities of said countries. The EDPS, Europol, Eurojust and the Secretariat of the Joint Supervisory Bodies were also involved, and the Article 29 Working Party was regularly informed about the developments. The EC also claims to have taken into account the results of the Spring Conference of the European Data Protection Authorities held in Krakow in April 2005. On 12 April and 21 June 2005, it attended meetings of the Police Working Party of the Conference of the European Data Protection Authorities; additionally it participated in a public seminar held by the Committee on Civil Liberties, Justice and Home Affairs of the EP, and declares to have taken into account the position of the EP, notably as set out in the EP recommendation to the EC and the Council on the exchange of information and cooperation concerning terrorist offences adopted on 7 June 2005.
[322] MEUWESE, *op. cit.*, p. 253.
[323] *Ibidem*, p. 254.

one with industry representatives) and a series of studies somehow similar to impact assessments that had been carried out.[324]

- European PNR

This impact assessment[325] was prepared notably by sending a questionnaire to the authorities of the different Member States and inviting them to discuss the answers at a meeting. The option identified as 'the preferred option' is said to "*provide better means of increasing security in the EU, while at the same time ensuring the better protection of data and minimising the costs for its setup and operation".*[326]

- Entry/exit system for external borders

A communication has been published on this issue by the EC, based on an impact assessment that was carried out with the support of two studies from external contractors.[327] The impact assessment[328] had suffered adaptations to take into account negative remarks[329] issued by the Impact Assessment Board. The entry/exit system had already been discussed in the impact assessment for the VIS, which concluded that its "*impact on fundamental rights, in particular the protection of personal data and privacy*" was "*exorbitant*",[330] but in the context of the new impact assessment it was alleged that changing circumstances justified a different conclusion.[331]

4.3. Monitoring the Design of Laws and Policies

Impact assessments are not the only tool in place to improve the drafting and discussing of EU legislative and policy proposals and their respect of fundamental rights. This section reviews first the general approach to fundamental rights conformity and its relevance for data protection, and, second, the contribution of data protection authorities to this process.

---

[324] In particular, a study form the Erasmus University commissioned by the Dutch government, another private Dutch, several studies of German origin and a study funded by the telecommunications industry.

[325] EC (2007), Accompanying document to the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Summary of the Impact Assessment, Commission Staff Working Document, SEC(2007) 1422, Brussels.

[326] *Ibidem*, p. 5.

[327] EC (2008), Communication from the Commission to the European Parliament and to the Council On an entry/exit system at the external borders of the European Union, facilitating of border crossing for bona fide travelers, and an electronic travel authorisation system, COM(2008)final, Brussels, p. 2.

[328] EC (2008), Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union": Impact Assessment, Commission Staff Working Document SEC(2008) 153, 13.2.2008, Brussels.

[329] Impact Assessment Board of the EC (2007), *Opinion on the Impact Assessment on the Communication on the creation of an entry/exit system at the external borders of the EU and on facilitating border crossing for bona fide travellers*, 4 December, Brussels.

[330] EC (2004), Commission Staff Working Document Annex to the Proposal for a Regulation to the European Parliament and to the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas: Extended Impact Assessment, SEC(2004) 1628, 28.12.2004, Brussels, p. 12.

[331] EC (2008), Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union": Impact Assessment, Commission Staff Working Document SEC(2008) 153, 13.2.2008, Brussels, p. 24.

4.3.1. Monitoring Compliance With Fundamental Rights

International and European human rights law has been an explicit reference for all EU developments directly related to data protection. The Data Protection Directive establishes a high level of protection for personal data in accordance with international law,[332] taking Convention No. 108 as a starting point. Its recital 10 specifically referes to Article 8 of the ECHR and to the recognition of privacy in the general principles of Community law.

In 2001, a requirement was imposed on the services of the EC to accompany all legislative proposals that could have an impact on fundamental rights with an indication that they were considered to be compatible with the requirements of the 2000 Charter,[333] which is self-binding for the EC since its adoption. References in legal texts and policy documents to compliance with fundamental rights are numerous.[334] In Directive 2002/58/EC, Recital 2 makes explicit reference to the respect of fundamental rights as recognised by the Charter of Fundamental Rights of the EU, notably in Articles 7 and 8.[335] Recital 11 of the same Directive states, however, that it addresses issues of protection of fundamental rights and freedoms only if related to activities governed by Community law, and therefore does not alter the existing balance of rights as established by the ECHR as interpreted by the ECtHR.

Sometimes the correctness of the proclaimed compliance with international law is unclear. The relation with international human rights instruments of the Data Retention Directive is particularly polemic. Since 2002, data protection authorities have voiced out that mandatory systematic retention of communications data for long periods can be considered an improper invasion of the fundamental right guaranteed by Article 8 of the ECHR. Moreover, some analysts have expressed that in their view Recital 27, in which compliance with the 2000 Charter is stated, might be considered 'paradoxical' and is in any case inaccurate.[336] Additionally, it has been highlighted that the development of third pillar legislation generally tends to disregard the consideration of compliance with the right to privacy as such, privileging references to compliance with data protection obligations in spite of the fact that no uniform data protection regime has ever been put in place in the third pillar.[337]

---

[332] GUTWIRTH, Serge (2002), *Privacy and the information age,* Rowman & Littlefield Publishers, Inc., p. 96.

[333] ALSTON, Philip and Olivier DE SCHUTTER (2005), *Monitoring Fundamental Rights in the EU: The Contribution of the Fundamental Rights Agency*, Oxford and Portland: Hart Publishing, p. 4.

[334] For instance, in EC's Green Paper on detection technologies in the work of law enforcement, customs and other security authorities there is an explicit reference to the need for the design, manufacture and use of detection technologies and associated technologies, together with legislation or other measures aiming to regulate or promote them, to fully comply with fundamental rights as provided for in the EU Charter of Fundamental Rights and the ECHR [EC (2006), *Green Paper on detection technologies in the work of law enforcement, customs and other security authorities*, COM(2006) 474 final, 1.9.2006, Brussels, p. 5].

[335] "This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter".

[336] RODOTÀ, Stefano (2006), "La conservación de los datos de tráfico en las comunicaciones electrónicas", *Revista de los Estudios de Derecho y Ciencia Política de la UOC* (IDP), N.°3.

[337] It has been argued that in the discussions on the establishment of SIS I, SIS II and Eurodac the right to private life as protected in Article 8 ECHR did not play an explicit role, even if the right to privacy was explicitly mentioned as being at stake in discussions at national level on certain issues [*When considering the protection of the rights of individuals, even if this was often referred to as "privacy rights", both negotiators and commentators focussed on the necessary safeguards as provided for in data protection law*" (BROUWER, *op. cit.*, pp. 128-129)]. The case was different with VIS (*ibidem,* p. 131).

4.3.2. The Role of Data Protection Authorities

Both the Article 29 Working Party and the EDPS are particularly sensitive to the role of human rights law in EU proposed legislation and policy options, and give particular attention to verifying that the EU respects fundamental rights in accordance with article 6 of the EU-Treaty. They also take special care in assessing whether proposed drafts are compliant with other obligations imposed to Member States, notably by the ECHR and Convention No. 108, which is binding on the Member States. Examples of such sensitiveness are numerous.[338]

The major reference point both for the Article 29 Working Party and the EDPS is the Charter and, more particularly, its Article 8 (on the right to data protection).The Article 29 Working Party can also refer to Article 8 of the ECHR (on the right to privacy), especially when assessing protection for processing activities not falling under the scope of the Data Protection Directive.[339] Additionally, the Working Party makes also reference sometimes to the observance of rights not directly related to the right to data protection or the right to privacy. For instance, it has explicitly referred to the content of Articles 3 and 18 of the International Convention on the Rights of the Child.[340]

The sources explicitly mentioned by the EDPS[341] as key for its screening of proposals are: (a) Article 8 of the EU Charter, with respect to the meaning and scope of the rights guaranteed by the ECHR, in particular its Article 8; (b) Community rules on the lawfulness of the processing of personal data, as included in Directive 95/46/EC, Regulation (EC) No 45/2001 and Directive 2002/58/EC; and (c) ECJ and ECtHR case law. Article 8 of the EU Charter is infallibly invoked in the preamble of EDPS opinions. Article 7 is sometimes mentioned by the EDPS in the opinions, especially as a subsidiary right to be invoked when the right to data protection cannot be called upon.[342]

4.4. Evaluations And Monitoring Of Laws And Policies

The evaluation of established laws and policies is believed to be potentially beneficial not only in order to improve them, but also to promote the transfer of learning among actors during the evaluation

[338] For instance, can be mentioned the following examples: the reservations voiced out by the Article 29 Working Party on the draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]", in Opinion 9/2004 (WP99); the check of compliance with Council of Europe Convention No. 108 undertaken by the EDPS in the *Second opinion on the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters,* where the EDPS states that solutions making the right to information dependent on a request by the data subject are not compatible with Convention No. 108.

[339] Article 29 Working Party (2007), Opinion 4/2007 on the concept of personal data, Adopted on 20 June, WP136, 01248/07/EN, p. 10.

[340] Article 29 Working Party (2005), Opinion on the use of location data with a view to providing value-added services, WP 115, November, 2130/05/EN.

[341] EDPS (2005), The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents, Policy Paper, 18 March, Brussels, p. 8.

[342] EDPS (2007) *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007)96,* 20 December, Brussels, p. 7.

procedure and, ultimately, to ameliorate policy-making.[343] Evaluation has been supported crucially for the development of the EU Area of Freedom, Security and Justice;[344] an ad-hoc EC communication defined evaluation as a tool aimed *inter alia* at further improving policies, programmes and instruments but also favouring learning and exchanges of good practice.[345] In this context, the EC proposed a distinction between 'monitoring implementation' and 'evaluation': the former shall consist in the continuous process of reviewing the progress of policies, while the latter shall include a discreet, punctual judgement of such policies according to results, impacts and needs. An example of one of the first evaluation initiatives launched in the Area of Freedom, Security and Justice was the economic evaluation of the Data Protection Directive undertaken in 2005.[346]

In practice, the evaluation of EU level laws and policies can overlap at least partially both with the monitoring of the drafting of new EU laws and policies (especially in the context of legislative reviews), and with the evaluation and monitoring of national measures implementing EU laws and policies. The review of the implementation of the Data Protection Directive, for instance, is in a sense an evaluation of a EU law, but it also encompasses an evaluation of Member States implementing measures, and it can as well be considered a measure preceding a legislative initiative or, in any case, preceding the policy choice of abstaining from preparing new legislative proposals.

Evaluation procedures as such are as a matter of fact sometimes very difficult to isolate from general monitoring practices, including practices such as the already examined consultations and impact assessments.[347] This section introduces some general mechanisms foreseen at EU level regarding the evaluation of law and policies (both at EU and national level), inasmuch as they concern the right to data protection, explains the role played by data protection authorities in this domain and explores other related relevant practices.

4.4.1. EC Obligations To Review And Report

A recurrent feature of EU legislation is the obligation to review the adopted provisions after a certain period of time (see also Section 4.1.1.). The Data Protection Directive contains a provision[348] requiring the EC to report to the Council and the EP at regular intervals[349] on its implementation, attaching to its report, if necessary, suitable proposals for amendments. In practice, Article 33 required the EC to report for the first time no later than 24 October 2001, but this deadline was not met. The EC launched a consultation in Summer 2002 and a report was published in 2003: the First report on the

[343] For a detailed discussion on evaluations in the area of freedom, security and justice, see: DE SCHUTTER, Olivier (2008), "The role of fundamental rights evaluation in the establishment of the area of freedom, security and justice" in MARTIN, Maik (ed.) (2008), *Crime, rights and the EU: The future of police and judicial cooperation*, a JUSTICE publication, pp. 44-88.

[344] The reason for this special relevance of evaluation is to be found on the different monitoring duties of the EC regarding, on the one hand, community legislation (in the context of which the EC can initiate infringement proceedings against Member States failing to comply) and, on the other hand, instruments adopted under Title VI of the EU Treaty concerning police and judicial cooperation in criminal matters (in the context of which there is no such possibility for the EC).

[345] EC (2006), Communication from the Commission to the Council and the European Parliament: Evaluation of EU policies on Freedom, Security and Justice, COM(2006) 332 final, 28.6.2006, Brussels, p. 2.

[346] Assessing the economic impact of the Data Protection Directive on data controllers, conducted carrying out interviews with data protection authorities: RAMBØLL MANAGEMENT (2005), *Economic Evaluation of the Data Protection Directive,* Final Report, May, Copenhagen.

[347] As expressed by the EC, systematic *ex-ante* appraisal greatly facilitates further interim and/or *ex-post* evaluation (*ibidem,* p. 95).

[348] Article 33 of Directive 95/46/EC.

[349] Starting not later than three years after the date referred to in Article 32(1).

implementation of the Data Protection Directive, of 15 May 2003,[350] containing a Work Programme for better implementation of the Data Protection Directive and a list of ten initiatives to be carried out in 2003 and 2004. In 2007, the EC issued a Communication to the EP and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. It was sent to the EDP, who reacted to the Communication with an opinion.[351]

The EC has been conducting a 'structured dialogue' with Member States on national transposition of the Data Protection Directive,[352] and performing comparative analysis of all the cases where wrong or incomplete transposition is suspected. Problematic issues can also be raised in complaints by citizens. Where a breach of Community law remains, the EC, as guardian of the Treaties, must open formal infringement procedures against the Member States concerned, and a number of such proceedings have already been opened.[353]

A statutory requirement in the electronic communications Framework Directive[354] also foresees its review.[355] Based partially on the results of different consultations, the EC proposed on November 13, 2007 a new review of the electronic communications regulatory framework. The Dublin and Eurodac Regulations also require the EC to report to the EP and to the Council of their application after three years of operation, proposing the appropriate amendments.[356]

4.4.2. The Role Of Data Protection Authorities

The essential mechanism in place to monitor the consistent implementation of EC data protection provisions in the Member States is the Article 29 Working Party. One of its functions is indeed to contribute to harmonised implementation, which in the view of its members does not only regard legal harmonization, but also harmonized enforcement. The Article 29 Working Party has taken initiatives to collect information on national enforcement practices, and it launched in 2004 a long-term program for an inventory of enforcement practices in the Member States.[357] The Working Party has not only the global responsibility of monitoring data protection needs in the Member States in general terms; it is also regularly mandated with concrete tasks of screening different aspects of implementation.[358]

---

[350] EC (2003), First report on the implementation of the Data Protection Directive (95/46/EC), Brussels, 15.5.2003, COM(2003) 265 final.

[351] EDPS (2007), Opinion on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 25 July, Brussels.

[352] EC (2007), Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, 7.3.2007, Brussels, p. 3.

[353] *Ibidem*, p. 5.

[354] Article 25 of the Framework Directive.

[355] It had to start no later than 25 July 2006.

[356] According to Article 24(5) of the Eurodac Regulation, the report should contain "an overall evaluation of Eurodac, examining results achieved against objectives and assessing the continuing validity of the underlying rationale as well as any implications for future operations". The EC published the Dublin Evaluation, the results of which were to feed into the process of evaluation of EU policies on Justice, Freedom and Security, as detailed in the Commission Communication of 28 June 2006, partially dealing with data protection. [Eurodac Supervision Coordination Group (2007), Report on the first coordinated inspection, 17 July, Brussels, p. 5-6].

[357] Article 29 Working Party (2005), Eight Annual report of the Article Working Party on Data Protection (covering the year 2004), adopted in November.

[358] An illustration of this sort of mandate concerns EC's policy on Privacy Enhancing Technologies (PETs): "The Commission thus calls on the Article 29 Working Party to continue its work in the field by including in its programme a permanent activity of analysing the needs for incorporating PETs in data processing operations as an effective means of ensuring respect for data protection rules" EC (2007), Communication from the

4.4.3. Other Practices

Sometimes, special initiatives are taken for the sake of the evaluation of laws and policies. For instance, an ad-hoc mechanism was launched to monitor the implementation of the Data Protection Directive 95/46/EC in relation to medical research and the role of ethics committees: the project Privacy In Research, Ethics and Law (PRIVIREAL),[359] an EC funded research project created to gather information regarding the implementation of the Directive across Europe.[360] Another interesting source of information potentially useful for evaluation is the EU Committee of the House of Lords, a committee active in the UK House of Lords. The information it collects for its different reports refers both to EU laws and policies and measures adopted or envisaged by the UK. Sub-Committee F (Home Affairs) of the Select Committee has issued a number of very well documented reports in the data protection field, which are all publicly available.[361]

Two singularly relevant practices for the gathering of information in the context of the evaluation of laws and policies are: (a) studies; (b) the direct collection of information by the Council; (c) the evaluation tool for EU policies on Freedom, Security and Justice.

a) Studies tendered by the EC

Studies can be tendered by the EC to external researchers and institutes, and are eventually made public.[362] They can be used by the legislator to support certain choices taken when drafting proposals;[363] however, comparative studies have been carried out also in fields in which eventually no legislative proposal was to be drafted.[364] Studies can also be tendered in the context of EC obligation to review and report on its own laws and policies.[365] Examples of subjects related to the protection of personal data for which the EC has tendered studies include: data protection and employment;[366] the

---

Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, 2.5.2007, Brussels, p. 7.

[359] More information at: http://www.privireal.org.

[360] The PRIVIREAL project terminated at the end of June 2005.

[361] House Of Lords, European Union Committee (2005), *European Union: Fifth Report*, European Union Committee Publications, Session 2004-2005, 22 February).

[362] Examples of studies: KORFF, Douwe (1998), *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*, Study Contract ETD/97/B5-9500/78, Commission of the European Communities, Final Report, October, Brussels (study tendered by Commission to examine the applicability of national data protection laws to legal persons, evaluate risks and make recommendations on possible improvements of the Data Protection Directive); RAAB, Charles et al. (1998), *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data: Test of the Method on Several Categories of Transfer,* University of Edinburgh, European Commission Tender No. XV/97/18D, September [this study did not precede a legislative proposal but interpretation of Article 25(2) of Directive 95/46/EC].

[363] The study on 'Unsolicited Commercial Communications and Data Protection' of January 2001 was used by the EC to argue in favour of a mandatory opt-in standard for unsolicited e-mail [KUNER, Christopher (2003), *op. cit.*, p. 27].

[364] Such is the case of the protection of the worker's personal data, already mentioned. [EC (2001), *Communication from the Commission: First stage consultation of social partners on the protection of worker's personal data* (retrieved from: http://ec.europa.eu/employment_social/labour_law/documentation_en.htm), p. 2].

[365] An example of this type of studies: HOGAN & HARTSON and ANALYSYS (2006), *Preparing the Next Steps in Regulation of Electronic Communications - A contribution to the review of the electronic communications regulatory framework*, Final Report, Study for the European Commission, July.

[366] FREEDLAND, Mark (1999), *Data protection and employment in the European Union: An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and its Member States, Oxford,* for the European

implementation of Directive 95/46/EC to sound and image data;[367] the options for and effectiveness of self-regulation in the information society;[368] the ways of setting an EU network on exchange of passenger name record (PNR) data;[369] privacy and trust in electronic communications.[370]

b) Collection Of Information By The Council

The Council can also contribute to evaluations by consulting different sources. The most technique it commonly uses is distributing questionnaires. Sometimes only Member State representatives are consulted using questionnaires distributed at Council level.[371] Questionnaires have in some occasions also been sent to national parliaments, including for instance questions on their involvement in the Prüm treaty and PNR US-EU agreement.[372] Collecting of information can take place for evaluation purposes, but also during discussions on policy or legislative proposals. In the third pillar, comparative studies as such are generally not undertaken before the drafting of proposals; this can potentially have a direct effect on the awareness of the EU legislator on the national legislations to be affected by its decisions,[373] unless the information is obtained differently.

c) Evaluation tool for EU Policies on Freedom, Security and Justice

In June 2006 the EC introduced a special evaluation tool for the EU Area of Freedom, Security and Justice, aimed to contribute among other things to better regulation and transparency of EU

Commission, Directorate-General for Employment and Social Affairs. This study was commissioned by the EC and was aimed to assess the convenience of having a data protection regime applying specifically to employment relationships, on the one hand, and the convenience of taken action at Community level. The researcher responsible for the study was an Employment Law professor from the University of Oxford who hoped that there would be a consensus in favour of a reporting and reviewing process at EU level.

[367] British Institute of International and Comparative Law (2003), *The implementation of Directive 95/46/EC to the Processing of Sound and Image Data*, Report, Service Contract CNS/2002/AO-7002/A/55, 16 May.

[368] Study tendered by EC DG INFSO to RAND Europe, aiming to support EC efforts to further these objectives by initiating and/or mediating self- and co-regulation. The evaluation was based on documentary, quantitative, 'elite interview' and electronic survey evidence. The findings and recommendations were validated by means of a key stakeholder workshop and an on-line survey (completed by 31 October 2007). Were accepted contributions from all internet users with knowledge of self-regulatory institutions.

[369] Under the title "B-Brussels: study on ways of setting up an EU network on exchange of passenger name record (PNR) data for law enforcement purposes": according to the notice of the tender, "*The study should analyse possible networks, and identify the most appropriate which could be set up, to exchange PNR data so as to ensure maximum work and cost efficiency, protection of personal data and security of such data during transmission and retention. The study should adopt a comparative approach between possible networks".* Notice number in OJ: 2007/S 66-079881 of 4.4.2007.

[370] WIK-Consult and RAND Europe (2008) *Comparison of Privacy and Trust Policies in the Area of Electronic Communications*, Final Report, Study for the European Commission, January.

[371] An example of answers from national delegations to a questionnaire can be found in: Council Of The European Union (2004), Note from the General Secretariat of the Council to the Working Party on Legal Data Processing on the Right to anonymity in the sphere of Legal Data Processing, 9370/04, 8 June Brussels. See also, on EC use of this possibility: EC (2006), Commission Working Document on the feasibility of an index of third-country nationals convicted in the European Union, COM(2006) 359 final, 4.7.2006, a document introducing some options for the design of the index and related questions for the Member States, distributed to the Council on 12 July 2006.

[372] Joint Committee Meeting at the initiative of the European Parliament and the Assembleia da República of Portugal (2007), The future of the EU as an area of Freedom, Security and Justice: Replies to a questionnaire to National Parliaments, European Parliament, Brussels.

[373] It has been the case for instance in regards to the Framework Decision on data protection for police and judicial matters [BUNYAN, Tony (2006), *The "principle of availability": Statewatch analysis*, December (retrieved from: http://www.statewatch.org/)].

activities.[374] The tool concerns directly data protection, as one of the policy sub-areas of Policy Area "Citizenship and fundamental rights" is "Fundamental Rights", in which the general objectives are to increase the awareness of fundamental rights amongst citizens, and to *"decrease instances of breaches of fundamental rights (including breaches of privacy, personal data protection and protection from violence against children, women and youth)"*[375]. Data protection authorities are mentioned in the section of 'indicators/evaluation questions' for outcomes: outcomes regarding the Data Protection Directive should be measured by "*appropriate enforcement mechanisms and remedies available to ensure respect for the law and assistance to individuals through: a) judicial remedies; b) intervention of data protection supervisory authority (ex officio or following complaints)*".[376]

4.5. Modulating the protection of personal data through research

A particular kind of interactions amongst actors takes place at EU level stimulated by EC-funded research programmes and initiatives. EC research funding can have modulating effects on relations between actors, and also contribute to develop certain policy choices.

4.5.1. EC Funded Research and Data Protection

EC funded research can be relevant for the right to the protection of personal data mainly for two different reasons: on the one hand, projects funded for other purposes might have a potential negative impact on the right to data protection; on the other hand, research can be expressly financed to encourage the development and uptake of tools promoting data protection, such as privacy-enhancing technologies (PETs). Currently, data protection is especially important in the context of the ICT and of the Security themes of the 7th Framework Programme (FP7) for research, as well as in the EU Framework Programme on 'Security and Safeguarding Liberties'.[377]

The ICT theme in FP7[378] is one of the two main financial instruments supporting the i2010 initiative, which is the EU policy framework for the information society. The other main financial instrument is the ICT specific programme within the Competitiveness and Innovation Programme (CIP), which runs for the years 2007-2013. One of the horizontal themes and actions of the ICT Policy Support Programme (PSP) are privacy protection infrastructures. This objective intends to set up a network bringing together partners that could contribute to a privacy protection infrastructure across a variety of information society areas.[379] ICT PSP Secretariat is at DG INFSO, while the CIP Secretariat is at DG Enterprise and Industry.

---

[374] EC (2006), Communication from the Commission to the Council and the European Parliament: Evaluation of EU policies on Freedom, Security and Justice, COM(2006) 332 final, 28.6.2006, Brussels, p. 12.
[375] Ibidem, p. 23.
[376] *Ibidem*, p. 28-29.
[377] The framework programme on "Security and Safeguarding Liberties" aims at ensuring an effective operational co-operation in the fight against crime and terrorism and strengthening their prevention, and consists of two financial instruments, titled 'Prevention of and fight against crime' and 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks'.
[378] An amount of 9.1 billion Euros have been committed for funding ICT research in FP7. Some 300 million Euro of the ICT budget have been dedicate to the "Future of Internet" theme, which is developed in different areas. The setting up of a European Future Internet Assembly has been launched [EC (2008), *The Future of the Internet: A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD*, DG Information Society and Media, p. 3]. One of the specific areas of the "Future of Internet" research funded deals with "Security, Privacy and Trust in the Future Internet".
[379] More concretely, the objective is to facilitate the emergence of an open European-wide trusted eServices market with dynamic compositions of services that reconciles different national privacy policies and offers user-

The EC did not fund any research on state or public security before 2004, as it was considered to be a national concern. However, the succession of a series of reports[380] from ad-hoc consultative groups lead to the establishment of a Security theme. The first of such groups was the Group of Personalities existing from 2003 to 2004; it was to be succeeded by the European Security Research Advisory Board (ESRAB)[381] (2005-2006) and then by ESRIF[382] (2007-2009), born as a public-private partnership with increased powers. EC funded Security research efforts have been severely criticised for insufficiently taking into account the need to balance interests; in particular, the development of the EU Security Research Programme has been criticised on the grounds that it was designed mainly to suit the interests of certain industrial sectors.[383]

Input to program or 'roadmap' research activities is sometimes obtained through consultation procedures or via the involvement of specific bodies.[384] Tools to coordinate research efforts are also put in place. European Technology Platforms (ETPs) bring together the main industry and academic research stakeholders in a particular field with the aim of better coordinating their research and related activities and achieving common goals. An important outcome of each ETP is a Strategic Research Agenda agreed by its members that also commit to its implementation. These Strategic Research agendas constitute an important input to the Work Programmes in FP7. The industrial and academic research stakeholders in ICT have already set up European Technology Platforms in nine ICT fields.

In July 2007, at the request of the EC, the EDPS reviewed some proposals submitted in the context of 7FP, answering the first call for tenders on ICT. Advice on data protection related aspects was provided on proposals that had already reached all thresholds and could be financed.[385] The EDPS has stated that his independency does not allow him to participate in EC funded projects, but considers that he could play a role in facilitating the cooperation between national or third country data protection authorities (in projects involving different Member States or third countries).[386] The EDPS

---

oriented technical means to allow the user to define privacy profiles, and to monitor and control their enforcement and propagation.

[380] Group of Personalities report "Research for a secure Europe" (March 2004), "European Security Research: The Next Steps" (September 2004), ESRAB report "Meeting the challenge: the European Security Research Agenda" (October 2006), "Fostering Public-Private Dialogue in Security Research and Innovation" (September 2007).

[381] The creation of ESRAB was recommended by the Group Of Personalities [EC (2007), *Commission Staff Working Document Accompanying document to the Communication from The Commission to the European Parliament and the Council on Public-Private Dialogue in Security research and Innovation: Impact Assessment*, SEC(2007) 1138, 11.9.2007, Brussels, p. 7].

[382] The creation of ESRIF was recommended by ESRAB (*idem)*.

[383] See: HAYES, Ben (2006), *Arming Big Brother: The EU's Security Research Programme*, TNI Briefing Series, No 2006/1, Transnational Institute: Amsterdam, April. The beginnings of the programme can be traced back to the establishment of a Group of Personalities in 2003 comprised of EU officials and some of EU's most important companies active in the field. The EC later obliged a "preparatory" budget for security research 2004-6, with the full European Security Research Programme to begin in 2007, and appointed an EU Security Research Advisory Board (ESRAB) to oversee the programme, on the Group of Personalities' recommendation. The EC could consult ESRAB on any questions relating to the content and implementation of the European Security Research Programme and ESRAB could make recommendations to the EC on: strategic missions and priority areas for security research, including FP7; implementation issues such as the exchange of classified information and intellectual property rights; on the use of publicly owned research/evaluation infrastructures; and on a communications strategy to promote awareness of the European Security Research Programme. On its recommendation, ESRIF was launched.

[384] The 2007-2008 work-programme defining the priorities for the calls for proposals to be launched in 2007 for the ICT theme research officially takes into account input from the Programme Committee, the IST Advisory Group (ISTAG), the European Technology Platforms in ICT and other preparatory activities including workshops with stakeholders [EC (2007), *Information and Communication Technologies (ICT) – A Theme for research and development under the specific programme "Cooperation" implementing the Seventh Framework Programme (2007-2013) of the European Community for research, technological development and demonstration activities, Work programme 2007-08*, C(2007)2460 of 11 June].

[385] EDPS (2008), *Annual Report 2007*, Brussels, p. 58.

[386] EDPS (2008), The EDPS and EU Research and Technological Development, Policy Paper, 28 April, Brussels, p. 3.

envisions his support to EC funded research as an indirect contribution to the implementation of the EU data protection regulatory framework, via a reinforcement of the application of the 'privacy by design' principle.[387] The Article 29 Working Party is generally not formally involved in the monitoring or performance of EC funded research activities, but has referred to EC funded research programmes in its opinions.[388]

4.5.2. Examples Of Research Activities

These are some examples of EC funded projects and initiatives related to data protection:

- Privacy and Identity Management for Europe (PRIME),[389] funded by the 6th Framework Programme. The project focused on demonstrating the viability of 'privacy-enhancing identity management'.[390] The PRIME Consortium taking care of the project consisted of 20 member organizations from industry, academia and research centers, as well as members of the research department of a data protection authority.[391] The PRIME Reference Group included external interested experts representing stakeholders such as EDRi, BEUC, or the Article 29 Working Party.

- e-PRODAT:[392] this project, partly financed by the EU and leaded by the Data Protection Agency of the Comunidad de Madrid, aims to promote the exchange of knowledge and experiences between public agencies and other public bodies concerning the protection of personal data used by governments and public administrations for the provision of public services.

- The Future of Identity in the Information Society (FIDIS)[393] is a Network of Excellence funded by the 6th FP, under Priority 2 'Information Society Technologies' (IST). It aims at developing a deeper understanding of how appropriate identities and identity management can contribute to a fair European information society. A total of 24 partners are part of the network, mainly but not only universities.

- EuroPrise[394], The European Privacy Seal: this project envisions a transparent European privacy certificate, a seal certifying privacy compliance with European data protection regulations. It is funded by the EC under the eTEN programme[395] and it is to end in November 2008. The consortium taking care of the project is lead by the Independent Centre for Privacy Protection Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz) and includes the participation of data protection authorities, private companies and research centers.

---

[387] *Ibidem*, p. 5.

[388] For instance, a series of projects are mentioned in Article 29 Working Party (2005), Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, WP 112, adopted on 30 September, 1710/05/EN: p. 7, mention of BITE, FIDIS, BIOSEC, BIOSECURE.

[389] More information at: https://www.prime-project.eu.

[390] For PRIME conclusions: LEENES, Ronald, Jan SCHALLABÖCK and Marit HANSEN (2008), *PRIME White Paper*, Final version, 15 May.

[391] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

[392] More information at: www.eprodat.org.

[393] More information at: http://www.fidis.net/.

[394] More information: http://www.european-privacy-seal.eu/.

[395] The eTEN programme finished in 2006. eTEN supported the deployment of trans-European e-services in the public interest. It aimed to accelerate the take-up of services to sustain the European social model of an inclusive, cohesive society. eTEN's six themes included eGovernment, eHealth, eInclusion, eLearning, Services for SMEs and Trust & Security.

- PRISE,[396] a Preparatory Action for Security Research: PRISE is the acronym for Privacy Enhancing Shaping of Security Research and Technology, a project launched under the motto 'A Participatory Approach to Develop Acceptable and Accepted Principles for European Security Industries and Policies'. PRISE was implemented to provide guidelines and support for security solutions with a particular emphasis on human rights, human behaviour and perception of security and privacy; it aimed especially to provide advice in the context of Security Research of the 7FP.

- ARTEMIS Joint Undertaking:[397] The purpose of this public-private partnership is to ensure a coherent and integrated implementation of European research efforts in the field of embedded computing systems, whilst promoting partnership between the Community, Member States and the private stakeholders in order to combine private with national and European public resources. The aim of the ARTEMIS Joint Undertaking is to achieve European leadership in embedded technologies, realising Europe's potential in the future markets for intelligent products, processes and services; while creating a single, Europe-wide research and development (R&D) programme and fostering R&D investments in the field.

- Examples of 7FP projects funded in the area of "Security, Privacy and Trust in the Future Internet" are the following: PRIMELIFE,[398] an Integrated Project (IP) focused on life-long privacy on the internet; PICOS,[399] a specific targeted research project on privacy and identity management for community services, and THINK-TRUST,[400] a "think tank for converging consumer needs in ICT trust, security and dependability" (coordination action).[401]

4.6. The Transatlantic Implementation Of Data Protection

The implementation of the right to data protection in the EU must deal with the reality of globalisation and massive and constant international data transfers. The provisions regulating data transfers to third countries are different depending on the type of data processing concerned. Processing in the context of activities falling under EC law ('first pillar') is regulated by the provisions of the Data Protection Directive, which establishes a special method to globally allow data transfers to third countries that have been recognised as providing 'adequate protection' for personal data. The general principle according to which no personal data can be transferred to third countries not ensuring an adequate level of protection is only familiar to a small percentage of EU population. During the last Eurobarometer survey, only 17% of the respondents stated that they had heard before that personal data could only be transferred outside the EU to countries ensuring an adequate level of protection.[402] Nevertheless, other possibilities to lawfully transfer data to third countries also exist.[403]

The transatlantic implementation of data protection has traditionally been a particularly difficult challenge for the EU. The US has never been recognised as generally ensuring 'adequate protection' for personal data. To reduce the potential negative impact of the Data Protection Directive, an ad-hoc

[396] More information at: http://prise.oeaw.ac.at.
[397] More information at: https://www.artemis-ju.eu/.
[398] More information at: http://www.primelife.eu.
[399] More information at: http://www.picos-project.eu/.
[400] More information at: http://www.think-trust.eu/.
[401] EC (2008), *The Future of the Internet: A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD*, DG Information Society and Media, p. 113.
[402] Figures ranged from 33% in Luxembourg and Hungary to 6% in Sweden [Gallup Organization (2008), *Data Protection in the European Union: Citizens' perceptions*, Analytical Report, Flash Eurobarometer 225, February, p. 33].
[403] For instance, based on individual consent or using standard clauses. See, on standard clauses: BENNET and RAAB, *op. cit.,* pp. 98-99.

solution was adopted, in the form of a Safe Harbour Agreement. The Safe Harbour Agreement establishes a hybrid, multilayered regime in which the EU set substantive data protection standards, US companies voluntarily commit to them, private and public bodies provide arbitration services, an US agency takes care of public enforcement, and the EC can terminate the whole agreement if compliance or public oversight in the US is considered deficient.[404] This innovative initiative has been described as a *co-regulatory* instrument.[405] It was originally strongly opposed by the Article 29 Working Party and the EP, which however lacked the institutional power to stop the EC from signing it.[406]

Data transfers to third countries do not follow the same rules when the processing does not fall under EC law: for transfers related to third pillar activities there is no uniform approach. The cases known as the 'PNR cases' (joined cases C-317/04 and C-318/04) famously illustrated the different regimes applicable, as well as the difficulties in determining which regime is applicable in certain circumstances, and notably when data originally collected for one purpose are to be processed for other purposes. The case concerned an agreement concluded between the EU and the US to allow for the processing by US authorities of PNR data of European passengers for law enforcement purposes; it was initially concluded as regarding 'first pillar' data processing, but the ECJ annulled the agreement[407] and a new one had to be concluded.

In 2007, a series of revelations regarding the screening by US authorities for law enforcement purposes of data concerning European financing transactions (known as 'the SWIFT affair') highlighted again the importance of ensuring data protection in the context of transatlantic transfers. The SWIFT affair led to specific negotiations between US and EU authorities, resulting in the introduction of a new 'supervisory' figure: the 'eminent European person', who shall be appointed to confirm that the US Terrorist Finance Tracking Program is implemented consistently with the related Representations for the purpose of verifying the protection of EU-originating personal data.[408] The 'eminent person' shall have appropriate experience and security clearances, and will be appointed for a renewable period of two years by the EC in consultation with the US Treasury Department. The 'eminent person' shall act in complete independence in the performance of his or her duties, and report findings and conclusions annually in writing to the EC; the EC will in turn report to the EP and the Council as appropriate. The US Treasury Department will give the 'eminent person' access, information and data necessary for the discharge of their duties.

In November 2006, in the context of discussions on the PNR agreement, and on the conclusion of agreements between the US and Europol and Eurojust, a EU-US High Level Contact Group was set up[409] to discuss about information sharing and protection of personal data processed for law enforcement purposes, and to act as an informal advisory group. It is composed of senior officials from the EC, the Council Presidency and the US Departments of Justice, Homeland Security and State, and it finalised its first report in May 2008.[410] The main idea presented in the report is the invitation to

---

[404] BENDRATH, Ralf (2007), *op. cit.*, p. 13.

[405] BENNET, Colin J. (2001), Privacy Self-Regulation in a Global Economy: A race to the top, the bottom or somewhere else?, paper prepared for Kernaghan Webb (ed.) January 31, p. 14.

[406] HEISENBERG, *op. cit.*, p. 8.

[407] The ECJ annulled both the EC decision asserting that US authorities provided 'adequate protection' for personal data processed in the context of the agreement, on the one hand, and the Council decision on the conclusion of the agreement, on the other hand.

[408] Office of Foreign Assets Control, US Department of the Treasury (2007), Publication of US/EU Exchange of Letters and Terrorist Finance Tracking Program Representations of the United States Department of the Treasury, Federal Register, Vol. 72, No. 204, 23 October.

[409] At the EU-US JLS Ministerial troika of 6 November 2006.

[410] Council of the European Union (2008), *Note from the Presidency to COREPER on EU US Summit, 12 June 2008 – Final Report by EU-US High Level Contact on information sharing and privacy and personal data protection*, 28 May, Brussels.

decide between continuing US-EU collaboration through a binding international agreement or through non-binding instruments such as ‘soft-law’ and a political declaration.

5. For A 'Reflexive' Assessment

This section firstly offers a brief introduction to the EU governance debate, and presents some reflections on decision-making regarding the protection of personal data developed in the context of such debate. Secondly, it presents the 'reflexive governance' approach, exploring the perspective's potential for a critical assessment of EU law- and policy-making regarding the right to the protection of personal data, focusing notably on the issue of 'representation'.

5.1. On the EU 'Governance' Debate and Data Protection

The REFGOV project expressly aims to contribute to the current debate on European governance taking as a starting point the idea that attempts to improve EU law- and policy-making by enhancing its legitimacy and effectiveness are based on divergent understandings of what is required to coordinate the different actors involved in the design and in the implementation of rules or policies. This sub-section brings to the fore some essential ideas discussed in the context of such debate.

The fields of EU studies and EU political discourse are probably two of the fields in which the term 'governance' has permeated more widely. EU studies have traditionally been very concerned with the perceived 'democratic deficit' of EU institutions. Until the 1990s, the 'democratic deficit' of the EU was generally discussed in terms of traditional 'government' theory, and tended to focus on the role of the different institutions and, especially, on the role of the EP. After the entry into force of the Maastricht Treaty in 1993, academic discourse focused progressively less on the 'government' debate to start privileging discussion in terms on 'governance', allowing for closer consideration of the contribution of different actors to reduce the mentioned 'democratic deficit'. At that time, some researchers had begun interpreting EU decision-making in terms of interactions between different territorial levels of power, through the notion of 'multi-level governance'. EU political discourse officially adopted the term 'governance' when the EC published its White Paper on European Governance, in July 2001.[411] The EC understanding of 'governance' was also related to a vision of 'multi-level governance', but it actually did not refer to different territorial levels of participation but to 'horizontal multi-level governance', in which different actors (including non-institutional actors such as 'civil society' organisations) play key roles. Five 'governance' principles were underlined in the White Paper: *openness, participation, accountability, effectiveness and coherence*; each principle is considered capital for establishing a more democratic governance.[412]

The 'governance' debate in the field of EU studies and EU political discourse cannot be completely disengaged from the so-called 'deliberative turn' undertook by democratic theory in the 1990s.[413] 'Deliberative democracy' explores the link between political decision-making and deliberations in the public sphere. Supporters of 'deliberative' and (closely linked) 'participatory democracy' theories have commonly framed the discussion on 'governance' in terms of enhancing the role of the 'civil society'.[414] Since 2000, the idea of 'civil society' participation as a way to improve both the efficiency and legitimacy of European governance is recurrent in EU policy discourses.[415] The notion of 'civil society', however, has been criticised on different grounds: it is principally argued that it seems to refer

[411] EC (2001), *European Governance: a White Paper*, COM(2001) 428 final, 25.7.2001, Brussels.
[412] *Ibidem*, p. 10.
[413] See: FINKE, Barbara (2007), "Civil society participation in EU Governance", *Living Reviews in European Gov*ernance, No. 2.
[414] See: SMISMANS, Stijn (ed.) (2006), *Civil Society and Legitimate European Governance*, Cheltenham: Edward Elgar.
[415] It has been asserted that both the EC and the ESC use the discourse on civil society and civil dialogue as an element of legitimisation for their activities and institutional position [SMISMANS, Stijn (2003), "European Civil Society: Shaped by Discourses and Institutional Interests", *European Law Journal*, Vol. 9, No. 4, September, p. 493].

to the representation of 'the citizen's' interests, while, in practice, provides only for 'expert representation'. In practical terms, the involvement of 'civil society' in EU decision-making has generally been rendered significantly difficult by the apparent non-existence of any organised 'civil society' at European level. This has lead to a debate on how to stimulate such EU-level organisation, or, in other terms, how to obtain the 'Europeanization of civil society'.

A notion closely linked to 'governance' is 'new governance'. This expression is generally understood as referring to a shift to non-hierarchical forms of law- and policy-making, to an increased used of soft-law, and, in general, to more easily adaptable forms of law.[416] The expression 'new modes of governance' refers to specific modes or techniques of governance allegedly reflecting the concerns of 'new governance'. Promoters of 'new modes of governance' believe that these modes are able to favour change by persuasion, monitoring and mutual learning. In the field of EU studies, some believe that 'new modes of governance' are modes opposed to the 'Community method' of EU decision-making, while others regard 'new modes of governance' as tools not opposed to but enhancing the 'Community method', and, finally, others consider that the opposition between 'new' and 'old' modes of governance might not be pertinent at all.[417]

Certain measures launched since 2000 by the EC have been particularly celebrated by those concerned with the 'governance' debate: the ways to involve 'stakeholders' in shaping the EU law and policy as described by the Governance White Paper; the development of integrated impact assessments; the adoption of the general principle and minimum standards for the consultation of interested parties by the EC, or the inclusion in the Draft Treaty establishing a Constitution for Europe of the principle of 'participatory democracy'. Those measures certainly fit clearly into to the 'Community method', and are in any case not opposed to it. Moreover, they can all be easily supported from a 'deliberative democracy' perspective. Much discussion on 'new modes of governance' has been focused on the development of the Open Method of Coordination (OMC), a governance technique put in place by the 2000 Lisbon European Council and widely interpreted as the 'third way' in EU governance (therefore opposed both to the 'Community method' and 'intergovernmental cooperation'). The interest of the OMC has been strongly emphasised by the supporters of the so-called 'democratic experimentalism' approach.[418]

The current situation of the right to data protection in the EU 'first pillar' can be considered to correspond to a hybrid scenario,[419] as it combines a binding framework directive (the Data Protection Directive) with 'new governance' or at least innovative governance approaches for implementation. Amongst the innovative tools put in place are to be highlighted not only those shared with other policy fields (such as integrated impact assessments, consultations, or public-private partnerships), but also other specific mechanisms such as the Article 29 Working Party or the EDPS. The role of data protection authorities in EU decision-making has already been studied with particular attention in the context of EU 'governance' discussions. It has been asserted that the particular mix of expertise,

[416] For a succinct description of the differences between notions of 'governance', 'new governance' and 'new modes of governance' in the context of EU studies, see: DE BÚRCA, Gráinne (2005), "New modes of governance and the Protection of Human Rights", in ALSTON, Philip and Olivier DE SCHUTTER (ed.), *Monitoring Fundamental Rights in the EU: The Contribution of the Fundamental Rights Agency*, Oxford and Portland: Hart Publishing, pp. 25-36.

[417] In this sense, see: TREIB, Oliver, Holger BÄHR and Gerda FALKNER (2005), *Modes of Governance: A Note Towards Conceptual Clarification*, European Governance Papers (EUROGOV) No. N-05-02.

[418] This approach is rooted in a peculiar understanding of 'deliberative democracy'; it considers especially relevant for democracy are 'decentralised implementation' of measures and gathering of information from dispersed actors. The OMC design fits well those requirements, as it establishes a series of networking decentralised decision-making units with a common benchmarking system that allows a more decentralised participation of the actors involved, in an apparently always dynamic and adaptable process [for this perspective, see: SABEL, Charles F., and Jonathan ZEITLIN (2007), *Learning from difference: the New Architecture of Experimentalist Governance in the European Union*, European Governance Papers (EUROGOV), No. C-07-02].

[419] DE BÚRCA, Gráinne and Joanne SCOTT (eds.) (2006), *Law and new governance in the EU and the US*, Oxford: Hart, p. 8.

delegated authority and network ties concentrated in the hands of data protection authorities might grant them the status of 'transgovernmental policy entrepreneurship', a term which stresses their impact on supranational decision making.[420] Researchers generally underline the process which allows independent authorities established at national and sub-national level to acquire a new, superior strength collaborating at EU level.[421] The situation in the third pillar, however, obliges to acknowledge only a limited validity to any assertion of the power of data protection authorities in EU decision-making in general terms.

5.2. The 'Reflexive Governance' Perspective

The 'reflexive governance' approach[422] is strongly linked to the mentioned discussions on EU governance.[423] The term 'reflexive' refers here to the 'reflexivity' that occurs when all the individuals bearing the consequences of a decision are involved in the making of the decision.[424] As this is acknowledged to be impossible as such, what is proposed is a 'second best solution' through the involvement of functional representatives or 'stakeholders', enhanced (and this is a key 'specificity of 'reflexive governance') with the systematic taking into account of the contextual dimensions of decisions, inviting decision-makers to always consider the effects of their decisions on other systems. This enhancement of the process would compensate for the impossible involvement of everybody in all decisions that could potentially have consequences on them.

One of the perspectives discussed in the context of the debate on EU governance has been 'reflexive deliberative polyarchy', which presents itself as a normative frame to identify a place for 'civil society' organisations in European governance.[425] The perspective builds on a defence of 'decentralised' political decision-making into lower-level units, in which citizens review their choices; information from those local experiments is pooled at a more central level, ensuring monitoring and encouraging mutual influence and learning, as well as reversibility of objectives and instruments. Building, moreover, on 'reflexive law' theory, 'reflexive deliberative polyarchy' reconsiders the role of law as an instrument to provide integration in society. Instead of providing substantial regulatory programmes, 'reflexive law' should according to this approach ensure that the subsystems are self-regulating without damaging the other subsystems. The 'reflexive governance' approach is certainly close to this perspective.

To phrase it in operative terms, it could be contended that the 'reflexive governance' point of view focuses on examining how to integrate those concerned by decisions in decision-making taking into

[420] NEWMAN Abraham (2008), "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", *International Organization*, 62, Winter, pp. 103-30. See also: EBERLEIN and NEWMAN, *op. cit.*.

[421] For a description of the Article 29 Working Party as an 'European concert of regulators' (and the distinction of this structure and 'decentralised integration' scenarios), see: CHITI, Edoardo (2003), "On European Agencies" in ERIKSEN Erik Oddvar, Christian JOERGES and Jürgen NEYER (eds.), *European Governance, Deliberation and the Quest for Democratisation*, Oslo/Florence 2003, ARENA Report 2/03.

[422] For an exploration of the theoretical framework of the approach, see: LENOBLE, J. and M. MAESSCHALCK (2006), *Beyond Neo-institutionalist and Pragmatist Approaches to Governance*, Working Paper Series REFGOV-SGI/TNU-1, Reflexive Governance in the Public Interest (REFGOV).

[423] See the Conclusions of Stijn SMISMANS in: SMISMANS, Stijn (ed.) (2006), *Civil Society and Legitimate European Governance*, Cheltenham: Edward Elgar.

[424] Therefore, it does not refer to the 'recursive' dimensions of decisions, which is another kind of 'reflexivity' that can be pointed out in governance discussions.

[425] On 'reflexive deliberative polyarchy' and its relationship with civil society, see: SMISMANS, Stijn (2007), "How political theory could deal with the role of civil society organisations in European governance: reflexive deliberative polyarchy", in RUZZA, Carlo and Vincent DELLA SALA (eds.), *Governance and Civil Society in the European Union: Normative Perspective*, Manchester: Manchester University Press.

account also the (other) interests of others. This leads to the formulation of two key questions related to the issue of representation: (a) Who are 'those concerned by decisions on the protection of personal data'?, and (b) who can/should/must represent them in EU decision-making?

(a) As the right to data protection of Article 8 of the EU Charter entitles 'everybody' to a series of rights towards their personal data, 'everybody' can be envisioned as a 'data subject' directly concerned by decisions on the right to the protection of personal data. By granting a series of rights to the 'data subject', however, Article 8 also imposes a series of obligations on those responsible for the processing of personal data, namely the 'data controllers'. Therefore, it could also be maintained by decisions regarding the right to data protection concern at least both 'data subjects' and 'data controllers'. The same Article 8, additionally, institutes the existence of data protection authorities, which are therefore also *directly* concerned with the development of the right to data protection. The Charter, finally, sets forth the right to data protection as a fundamental right, and it might be argued that all actors, and especially all institutional actors, shall be 'concerned' by fundamental rights and, consequently, also by data protection.

(b) Who can/should/must represent the concerns of 'those concerned'? On the one hand, it could be reasoned that inasmuch as data protection authorities embody the defence of the right to the protection of personal data, they inevitably must represent both the interests of 'data subjects' and 'data controllers', as well as their owns. On the other hand, it could also be supported that the rationale behind the existence of data protection authorities (and, actually, behind the very existence of data protection legislation) is grounded on a need to re-balance an imbalanced power situation: according to this perspective, the role of data protection authorities and of data protection legislation is to act in favour of 'data subjects' in front of 'data controllers' (which are already empowered by the capabilities of technologically assisted data processing). Do data protection authorities need to portray a balanced approach, or are they entitled (or obliged) to take a more partial perspective? In practice, data protection authorities tend to be attributed an ambivalent role: they can be regarded as a sort of 'impartial' advocate of the right to data protection, but they can also be integrated in the decision-making process to 'counter' forces tending to privilege the interests of 'data controllers'. Independently of the role attributed to data protection authorities, there is in any case no reason to understand that the data subjects' concerns regarding the protection of personal data are to be exclusively placed on their hands. Indeed, such representation inevitably coexists with other forms of representation: the 'traditional' democratic representation, and functional representation. The unstable role played by data protection authorities might have as a side effect an impact on the role attributed to other actors. In a sort of 'paternalistic' attitude, data protection authorities might tend to position themselves as the best interlocutors on data protection concerns. This could help explaining why bodies such as the Article 29 Working Party or the EDPS, despite their contributions to decision-making regarding data protection, have done little to improve decision-making processes in a way that they encourage 'civil society' active involvement.

6. Proposals

Taking into account the assessment introduced, a series of paths for reflection and improvement have been identified. Opportunities to develop and implement new strategies might appear in a not too distant future, especially as some signs appear to announce that the EC and other involved actors are considering with great attention the possible need to review the Data Protection Directive. In this sense, the EC divulged in April 2008 its intention to award a contract for the development of a comparative study on different approaches to new privacy challenges, in particular in the light of technological developments.[426] The EDPS has stressed the convenience for interested discussants to have a clear indication of a possible date for the eventual review.[427]

6.1. The Data Subject As Starting Point

As the right to data protection is structurally indebted to the notion of a 'data subject' disadvantaged in the power imbalance created by data processing practices, the main priority when rethinking law and policy-making regarding the protection of personal data should be to consolidate the positive subjective rights granted to the individual. This forces to consider with detail who represents and how are represented the interests of the 'data subject' regarding data protection when decisions are taken.

The use of the expression of 'user empowerment', recurrent in ICT discourse, as well as the motto of 'empowering the citizen', common in EU political discourse, might express some parallel concerns. The category of 'data subjects', however, is wider than those of 'users' and 'citizens': 'data subject' can be *everyone* whose personal data are processed, regardless of its status as user or non-user, citizen or non-citizen.

6.2. The Myth of the 'Informed Data Subject' v. The 'Average Consumer'

Consumer protection law acknowledges an unbalanced power relation between consumers, on the one hand, and providers of services and products, on the other hand. Consumer law aims at restoring the balance to prevent providers from taking unfair advantage of it. Data protection's strategy to protect the citizen is slightly different: protection can be partially lifted through the data subject's consent to the processing of personal data. The limitations of such consent can render the protection only theoretical. Should the modalities of consent be better framed, to guarantee that it remains a protective tool in the hands of the 'data subject' instead of a legitimizing instrument at disposal of 'data controllers'? There might be lessons to be learned from consumer law's notion of 'average consumer', who is not always fully informed. To ensure that consent is duly implemented and can be effectively used, the limits of un-fair solicitation of consent to the processing of personal data need to be rendered explicit.

This seems especially relevant as business models tend to rely increasingly on providing 'free' services in exchange for personal data. There have actually already been calls backing an approach to right to privacy and the protection of personal data framed in terms of consumer protection.[428] The

---

[426] Directive 95/46/EC entered into force on 24 October 1998. EC's first report on its implementation concluded in 2003 that no legislative changes were required, but established a work programme for better implementation. The EC published a communication on the follow-up of the work programme in March 2007, underlining only 'minor' problems believed not to justify legislative proposals.

[427] HUSTINX, Peter (2008), *Strategic challenges for data protection in Europe*, speech delivered at the 9th Data Protection Conference, 6 May, Berlin, p. 3.

[428] POULLET, Yves and Jean-Marc DINANT (2004), L'autodétermination informationnelle à l'ère d'Internet: Eléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif (T-PD), Rapport

EC adopted on November 2007 a proposal to amend Directive 2002/58/EC that foresees to ensure collaboration with the consumer protection cooperation network, even if only for better protection against spam. In December 2008 shall be published an EC Communication presenting a Guide on rights and obligations of users in the information society, which is a follow-up of an EP Resolution of June 2007 requiring the EC to present a Charter of user rights in relation with digital content. All these steps look as steps in a promising direction.

6.3. Consistent Independence And Powers Of Data Protection Authorities

National administrations should carefully guarantee the independence of data protection authorities, and make sure that they enjoy the necessary powers to ensure effective compliance. As current implementation of the Data Protection Directive seems to provide neither consistent independence, nor harmonised practices, there might be good reasons for a revision of relevant provisions.

Independence from governmental authorities and from 'data controllers' is not only important to ensure impartial monitoring of processing practices. The independence of data protection authorities is also crucial for their legitimacy, especially important as they enjoy an enhanced role in EU decision-making. Civil society representatives have more than once explicitly backed the reinforcement of data protection authorities, mainly regarding their independence and resources.[429] The reinforcement of data protection authorities should also encompass their powers. Lack of powers to effectively enforce data protection affects also their individual credibility, but also their joint power at EU level. If data protection authorities do not have the capability or the habit of ensuring effectively compliance at national level, a group like the 29 Working Party could over the long haul increasingly resemble *any other* EU level consultative body.

6.4. Mainstreaming Data Protection In Public Administration

One of the main challenges for the future of data protection in the EU is the development of e-government.[430] The challenge of developing e-government practices while ensuring effective data protection concerns all public administrations, and the EU can possibly play an important role to disseminate best practices in this area. The experimental approach of the EDPS seems a key factor in this context.[431] It enjoys a pivotal position derived from its different cooperation duties, which can be very useful for the transfer of learning between different actors.

The data protection officers' model might be worth special attention. It changes the paradigm of data protection supervision from external to internal monitoring, and can have a series of particular advantages. The Article 29 Working Party has already expressed its views on the possible generalisation of data protection officials, "*that is, shifting from administrative to internal supervision*",

---

sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, Strasbourg, 18 novembre, p. 59.

[429] See, for instance: Ligue des Droits de l'Homme (2006), *Carte d'identité électronique: Penser le progrès au lieu de le subir…* , Commission Justice, Mai.

[430] The issue of data protection and e-government has notably been addressed in the UK after recent security breaches related to personal data. There have been calls to ensure that a culture of respect for personal data is fostered, with particular reference to the possible obligation to carry privacy impact assessments at an early stage of Government projects as well as the need to take action to foster a positive culture for the protection of personal data by public sector bodies [House Of Lords / House Of Commons Joint Committee On Human Rights, (2008), *Data Protection and Human Rights,* Fourteenth Report of Session 2007-08. HL Paper 72, HC 132, London: The Stationery Office Limited, 14 March, p. 3].

[431] See also on the potential contribution of the EDPS to 'privacy compliant' e-Government: POULLET, Yves (2006), "The Directive 95/46/EC: Ten years after", *Computer Law & Security Report*, 22, p. 209.

which it encourages.[432] The tool of 'prior checking', in a sense reminiscent of PIAs, is also being interestingly refined by the EDPS.

6.5. Is The EU taking Privacy 'Too Personally'?

The research has highlighted a discourse gap between data protection authorities, strongly focused on the defence of the fundamental right to the protection of personal data, and 'civil society' organisations, much more concerned with the protection of the fundamental right to privacy. If data protection authorities have been able to effectively push for the recognition of the right to data protection as a European fundamental right at the highest level it is, at least partially, as a result of their strong focus on the right to data protection, as well as of their will to clearly differentiate it from the right to privacy. There might be a risk, however, that the right to the data protection is developed to the detriment of the right to privacy. Additionally, as the different duties and powers of data protection authorities are structurally dependent on the very definition of 'personal data',[433] which marks also the limits of the scope of application of data protection law, there is a risk of seeing the extension of such definition transformed into a power issue.

The EC does refer regularly to 'privacy', but not always to 'privacy' exactly *as in 'the right to privacy'*. In a sort of rhetorical move possibly meant to mark clearly the boundaries of its competences in front of the competences of DG JLS, DG INFSO has been particularly generous with the use of the term 'privacy'. Paradoxically, except for a few cases in which there seems to be a clear reason to use 'privacy' rather than 'data protection',[434] the protection granted is much more reminiscent of the positive approach of data protection than of right to privacy: such is the case for instance of notions such as '*user-centric privacy*', or of many practices referred to with the expressions of *privacy*-by-design, *privacy*-enhancing technologies (PETS), or *privacy*-enhancing identity management.

6.6. A disconnected 'civil society'?

The situation concerning 'civil society' organisations involved or potentially involved in representing data protection concerns at EU level appears to suffer from two main problems. Organisations mainly focused in defending the right to the protection of personal data are not coordinated at European level, or only very loosely, while amongst the actors most regularly involved in EU decision-making some Member States appear to be over-represented, and many are remarkably underrepresented.

EU institutions are particularly well placed to encourage the transfers of learning supporting and stimulating an enhanced involvement of 'civil society' actors. The idea of the EC helping stakeholders to acknowledge their fundamental rights in consultations during impact assessments is especially interesting in this context. Data protection authorities might also have a key role to play. Until now, their initiatives to support 'civil society' have been limited, especially at international level.[435] The recently established EU Agency for Fundamental Rights could, maybe, boost new dynamics.

---

[432] Article 29 Working Party (2005), Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union, WP 106, adopted on 18 January, 10211/05/EN, p 23.

[433] For the EDPS, see Article 41(2) of Regulation No 45/2001.

[434] For instance, when describing Directive 2002/58/EC, known as the e-Privacy Directive, as it does cover more than the mere processing of personal data (notably, the confidentiality of communications).

[435] The International Conference of Data Protection and Privacy Commissioners welcomed and financially supported in its 2007 edition an official meeting of civil society representatives. It is unclear whether the initiative will be repeated.

6.7. Avoiding The Use Of Special Techniques To Feed Circular Processes

The 'reflexive governance' approach advocates the participation of those concerned by decisions in the decision-making process, but stresses that such decision-making should take into account the concerns of all those potentially affected by the decisions, and not only of those participating in decision-making. There is certainly a risk in using mechanisms relying on the input from interested parties to adopt and implement policies, as they might be tempted in designing policies and/or new decision-making processes that mainly benefit the interested parties involved. The crystallization of input from 'stakeholders' in stable 'consultative' bodies might contribute to increase this risk. Research funding appears to be particularly vulnerable at the moment, especially as data protection authorities and 'civil society' do not seem to be fully involved in key stages of the decision-making process. Their input should not be limited to ensuring compliance with the right to data protection, but cover its promotion.

6.8. International And Multi-actor Cooperation

There is a need to develop effective protection of personal data globally, despite dissimilarities amongst institutional frameworks. The OECD has acknowledged the benefits of cooperation for international enforcement in an ad-hoc recommendation published in 2007, *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*.[436] The recommendation suggest that countries should encourage 'privacy enforcement authorities'[437] to consult with criminal law enforcement authorities, privacy officers in public and private organisations and 'civil society' and businesses *"in particular in helping raise awareness among individuals on how to submit complaints and obtain remedies*".[438]

In contrast to this approach, the international implementation of data protection provisions appear to be often negotiated through processes offering very low degrees of openness and almost non-existent possibilities for involvement of data protection authorities or 'civil society' representatives. Over the years, the EU has developed a rich even if asymmetrical institutional framework to monitor and favour data protection in internal EU decision-making, relying not only on the main EU institutional actors, but in a myriad of actors. There might be no justification to sideline some players as soon as demands to reduce the protection of personal data are voiced out by third country representatives.

[436] In the context of the OECD, the term 'privacy' generally refers to the protection of personal data as understood in the EU.
[437] Defined as "any public body, as determined by each Member country, that is responsible for enforcing Laws Protecting Privacy, and that has powers to conduct investigations or pursue enforcement proceedings" (§1, Organization for Economic Co-operation and Development (OECD) (2007), Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, adopted by the OECD Council on 12 June).
[438] Idem.

7. Conclusions

The thematic research has reviewed the main actors and current practices relevant in the context of EU law- and decision-making with respect to the protection of personal data. Moreover, it has explored a way to assess them from the perspective of 'reflexive governance'. In order to allow for such an assessment, it sustains that the 'reflexive governance' approach might be understood as the search for modes of decision-making that organize the involvement of actors concerned by the rules and policies which will affect them in the design and the implementation of such rules and policies, taking into account, furthermore, the contextual dimension of such decision-making.

The main findings resulting from the thematic research can be divided into two themes: (1) the issue of representation (who is entitled to represent 'those concerned by data protection'?) and (2) the modes of decision-making, an issue that can be sub-divided into three basic questions: (a) how to involve 'those (representing) those concerned by decisions on data protection'?; (b) how to take into account the (other) concerns of the others when taking decisions on data protection?, and (c) what happens when data protection is (or is not, but should be regarded as) an external concern in decision-making?

(1) Regarding the issue of representation, have been described different possible interpretations of who is concerned by the right to data protection and who is entitled to represent them. The divergent interpretations can have practical consequences on decision-making, notably affecting the levels of engagement in certain activities by data protection authorities and their relations with other actors. In this sense, for instance, the EDPS can consider that its independence does not allow for active implication in research activities, while other data protection authorities do actively participate. The search for a balanced approach can be perceived as an ambiguous attitude by some 'civil society' organisations fully committed to the defence of the 'data subject' point of view. The role attributed to the different actors by EU institutions is variable: while in the context of certain procedures the EC regards data protection authorities as trustworthy, it can also broadly neglect their input on other issues. Ultimately, different perceptions might be considered at least partially as symptomatic of different understanding of fundamental rights, as well as of the nature of the right to data protection.

(2) Concerning the modes of decision-making, at first glance the most striking feature is certainly the divergent realities of first pillar and third pillar data protection. The pillar division marks different degrees of homogenisation and different decision-making procedures: 'harmonisation' in the first pillar versus intergovernmental cooperation in the third pillar; active participation of the Article 29 Working Party in the first pillar, and absence of an equivalent body in the third pillar. The pillar division illustrates also the limitations of the recognition of data protection as EU wide fundamental right, due to special considerations regarding data protection and national security, as well as opt-outs or special interpretations of the Charter. Institutionally, the different scenarios encapsulated by the draft Constitutional treaty and by the Lisbon treaty have only allowed for moderate optimism for a reinforcement of the recognition of the right to data protection.

A deeper analysis reveals that inter-pillar asymmetries are only one type of forces determining decision-making modes related to data protection. Another, possibly more relevant type of tensions is created by the internal division of tasks amongst EC services. The Units dealing with the two most important legal instruments of EU data protection, namely the Data Protection Directive and the e-Privacy Directive (the provisions of which "*particularise and complement*"[439] those of the Data Protection Directive) are part of two separate Directorate-Generals, respectively DG JLS and DG INFSO. Both directorates can apply very different procedures for allegedly similar purposes: for instance, the progress on data protection at national level in the context of the scope of competences of DG JLS is evaluated through the evaluation tool for EU Policies on Freedom, Security and Justice, while the progress on data protection in the information society is measured in the context of the reviews of the i2010 initiative.

[439] Article 1 of Directive 2002/58/EC.

(a) How to involve those (representing) 'those concerned by decisions on data protection' in EU decision-making? EU institutions might fail to offer a clear explanation on the assumptions on which they base different tools and mechanisms to stimulate involvement, but it is undeniable that they do develop such tools and mechanisms. The number of actors created, supported and/or financed is notable, as is the number of different shapes that they can adopt: agencies, working parties, joint authorities, expert groups, independent expert groups, stakeholders groups, research consortiums, reference groups of research consortiums, platforms, or joint undertakings. Additionally, institutions punctuate decision-making processes with a series of intertwined tools and mechanisms: integrated impact assessments, consultations, comparative studies, pre-screening, post-evaluation and periodical reviews, amongst other procedures, can create a sort of continuum favouring discussion and negotiation of different concerns. Such tools and mechanisms can play an especially useful tool for the defence and the promotion of data protection by offering opportunities to introduce such concerns at different stages of policy-making [(c)]. In this continuum, however, the particular effectiveness of involvement is not always easy to determine.

The EDPS appears to play a crucial role in this context. Its proactive attitude towards (extremely close) monitoring and promoting data protection transform it into a unique body, offering unparalleled possibilities to play a relevant role during almost all the policy-cycle. Its pivotal (and inter-pillar) position is also capital for the transfer of learning. Nevertheless, the EDPS has still many challenges to address, such as how to ensure monitoring of developments with a strong impact on EU data protection that escape 'normal' institutional procedures (for instance, in the context of international negotiations on data protection, or through originally extra-EU initiatives such as Prüm), or how to improve the defence and promotion of data protection in the context of research funding.

(b) How to take into account the (other) concerns of the others when taking decisions on data protection? It could be argued that the Reform Treaty envisages with special care an answer to this question, as it foresees an explicit reference to 'security concerns' to be taken into account when regulating data protection. With such an obligation, nevertheless, what is revealed is an assumption according to which data protection might be potentially regulated without duly taking into account other concerns, as well as a particular perspective on how to integrate data protection in the construction of EU 'public interest',

The research has proposed eight paths to guide reflection towards future improvements: taking the data subject as the starting point; applying principles of consumer law to the protection of personal data; reinforcing the independence and powers of data protection authorities; mainstreaming data protection in public administration; critically reviewing the relation between the development of the right to data protection and the right to privacy; re-thinking 'civil society' for data protection; avoiding the use of techniques to legitimise circular decision-making; and improving international and multi-actor cooperation.

Ultimately, the research has highlighted that different assumptions on representation regarding data protection can themselves be indicative of different implicit assumptions on the nature of fundamental rights, as well as on the role that they are to be attributed in the construction of the 'public interest'. Consequently, it appears that any development of a 'reflexive governance' approach for fundamental rights law and policy-making should not neglect a critical assessment of the issue of representation.

8. Bibliography

6.1 General references

ADAM, Alexandre (2006), "L'échange de données à caractère personnel entre l'Union européenne et les Etats-Unis: Entre soucis de protection et volonté de coopération", *Revue Trimestrielle du Droit Européen,* 42(3), juillet septembre.

AGOSTINI, Aldo (2006), *Biometria e privacy: i presunti nemici a confronto - Guida Pratica,* Bologna: EDIS Edizioni Specializzate SRL.

ALLIO, Lorenzo (2007), "Better regulation and impact assessment in the European Commission", in KIRKPATRICK, Colin and David PARKER, *Regulatory Impact Assessment: Towards better regulation?*, Edward Elgar, pp. 72-105.

ALSTON, Philip and Olivier DE SCHUTTER (2005), *Monitoring Fundamental Rights in the EU: The Contribution of the Fundamental Rights Agency*, Oxford and Portland: Hart Publishing.

ANDENAS, Mads and Stefan ZLEPTNIG (2003), "Surveillance and Data Protection: Regulatory Approaches in the EU and Member States", *European Business Law Review*, Volume 14, n°6.

ARENAS RAMIRO, Mónica (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia: Tirant Lo Blanch.

Article 29 Working Party (Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data) (2005), *Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, WP 112, adopted on 30 September, 1710/05/EN.

---- (2005), *Eight Annual report of the Article Working Party on Data Protection (covering the year 2004),* adopted in November, European Communities.

---- (2005), *Opinion on the use of location data with a view to providing value-added services,* WP 115, November, 2130/05/EN.

---- (2006), *Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the e-Privacy Directive,* WP 126, 26 September.

---- (2007), *Opinion 4/2007 on the concept of personal data*, adopted on 20th June, WP136, 01248/07/EN.

---- (2008), *Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)*, WP 147, 18 February.

---- (2008), *Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive),* WP150, 15 May.

BENDRATH, Ralf (2007), *Privacy Self-Regulation and the Changing Role of the State: from Public Law to Social and Technical Mechanisms of Governance*, TranState Working Papers, No. 59, Sfb597, Staatlichkeit im Wandel / Transformations of the State, Bremen.

BENNET, Colin J. (2001), *Privacy Self-Regulation in a Global Economy: A race to the top, the bottom or somewhere else?*, paper prepared for Kernaghan Webb (ed.), 31 January .

BENNET, Colin J., and Charles D. RAAB (2006), *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge, Mass.: The MIT Press.

BEUC (2007), *Letter to Ms Neelie Kroes (European Commission) on the Proposed acquisition of DoubleClick by Google,* 27 June.

BIAGINI, Cédric and Guillaume CARNINO (2007), *La tyrannie technologique: Critique de la société numérique,* Editions l'Echappée.

BIGNAMI, Francesca (2005), "Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network", *Michigan Journal of International Law*, 26, pp. 807-868 (retrieved from: http://eprints.law.duke.edu/archive/00001560/01/26_Mich._J._Int'l_L._807_(2005).pdf).

BOLKENSTEIN, Frits (2002), *Answer on behalf of the European Commission dated from 26/09/2002 to: "*Written Question E-1723/02 by Bart Staes (Verts/ALE) to the Commission: The protection of privacy and electronic data processing", OJ C 052 E, 06/03/2003, pp. 97-99.

British Institute Of International And Comparative Law (2003), *The implementation of Directive 95/46/EC to the Processing of Sound and Image Data*, Report, Service Contract CNS/2002/AO-7002/A/55, 16 May.

BROUWER, Evelien (2006), *Digital Borders and Real Rights: Effective remedies for third-country nationals in the Schengen Information System*, Centre for Migration Law, Radbourd University Nijmegen: Nijmegen.

BRULIN, Hughes (2003), "La protection des données: quête et errements dans le Troisième Pilier", *Actualités de Droit Pénal Européen*, Bruxelles: La Charte, p. 137.

BUNYAN, Tony (2007), "EU: Cementing the European State – new emphasis on internal security and operational cooperation at EU level", Statewatch Bulletin, vol. 17, 3/4, October.

BYGRAVE, Lee A. (2002), "The 1995 EC Directive on data protection under official review – feedback so far", *Privacy Law & Policy Reporter*, volume 9, pp. 126-129.

---- (2002), "Privacy-Enhancing Technologies: Caught between a Rock and a Hard Place", *Privacy Law & Policy Reporter*, volume 9, pp. 135-137.

CHITI, Edoardo (2003), "On European Agencies" in ERIKSEN Erik Oddvar, Christian JOERGES and Jürgen NEYER (eds.), *European Governance, Deliberation and the Quest for Democratisation*, Oslo/Florence 2003, ARENA Report 2/03.

CIS Joint Supervisory Authority (2005), *Opinion to the Council of the European Union on Supervising the Customs Information System*, 4 March 2005, 7106/05, Brussels.

Committee on Citizen's Freedoms and Rights, Justice and Home Affairs of the European Parliament (2004), *Report on the First Report on the implementation of the Data Protection Directive (95/46/EC) ,* Rapporteur: Marco Cappato, 15-0104/2004 EN, 24 February.

Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (2007), *Report on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation),* Rapporteur: Martine Roure, A6-0205/2007, 24 May.

Commission nationale de l'Informatique et des Libertés (CNIL) (2007), *27e Rapport d'activité 2006,* La Documentation Française : Paris.

Council (2004), *Note from the General Secretariat of the Council to the Working Party on Legal Data Processing on the Right to anonymity in the sphere of Legal Data Processing*, 9370/04, 8 June, Brussels.

Council Of Europe (1973), *Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector*.

---- (1974), *Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector*.

---- (1987), *Recommendation No. R(87)15 concerning the use of personal data in the police sector*, adopted by the Committee of Ministers on 17 September 1987.

Council of the European Union (2007), *Presidency Conclusions, Brussels European Council 21/22 June 2007,* 23 June, 11177/07, Brussels.

---- (2008), *Note from the Presidency to COREPER on EU US Summit, 12 June 2008 – Final Report by EU-US High Level Contact on information sharing and privacy and personal data protection*, 28 May, Brussels.

DE BÚRCA, Gráinne (2005), "New modes of governance and the Protection of Human Rights", in ALSTON, Philip and Olivier DE SCHUTTER (ed.), *Monitoring Fundamental Rights in the EU: The Contribution of the Fundamental Rights Agency*, Oxford and Portland: Hart Publishing, pp. 25-36.

DE BÚRCA, Gráinne and Joanne SCOTT (eds.) (2006), *Law and new governance in the EU and the US*, Oxford: Hart.

Declaration of Civil Society Organizations On The Role of Data Protection and Privacy Commissioners (2007)*,* Montreal, September 25.

DE SCHUTTER, Olivier (2005), "Article II-68 – Protection des données à caractère personnel", in L. Burgorgue-Larsen, A. Levade, F. Picod (eds.), *Traité établissant une Constitution pour l'Europe. Commentaire article par article*, Bruxelles: Bruylant, p. 147.

---- (2008), "The role of fundamental rights evaluation in the establishment of the area of freedom, security and justice" in MARTIN, Maik (ed.) (2008), *Crime, rights and the EU: The future of police and judicial cooperation*, a JUSTICE publication, pp. 44-88.

DIGITAL WATERMARKING WORKING GROUP (2005), Digital Watermarking Working Group's Response to Privacy Concerns Raised by Paper WP 104 from the European Union's Data Protection Working Party (Response to EU Paper WP 104), Digital Watermarking Alliance, 31 March.

EBERLEIN, Burkard and Abraham NEWMAN (2008), *Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union*, Governance, vol. 21 (1), pp. 25-52.

EDRI-Gramm (2005), "EC: data protection inadequate in Austria and Germany", *EDRI-GRAMM Newsletter*, Number 3.17, 24 August, (retrieved from: http://www.edri.org/edrigram/number3.17/DPA)].

Electronic Privacy Information Centre (EPIC), *Privacy & human rights 2006: an international survey of Privacy laws and Developments*, EPIC and Privacy International.

EURODAC Supervision Coordination Group (2007), *Report on the first coordinated inspection*, 17 July, Brussels.

European Commission (EC) (1973), *Community Policy on Data Processing. Communication of the Commission to the Council,* SEC (73) 4300 final, 21 November.

---- (2001), *Communication from the Commission: First stage consultation of social partners on the protection of worker's personal data* (retrieved from: http://ec.europa.eu/employment_social/labour_law/documentation_en.htm).

---- (2001), *European Governance: a White Paper*, COM(2001) 428 final, 25.7.2001, Brussels.

---- (2002), *Second stage consultation of social partners on the protection of workers' personal data*, 31 October.

---- (2002), *Communication from the Commission "Towards a reinforced culture of consultation and dialogue – General principles and minimum standards for consultation of interested parties by the Commission*", COM(2002) 704 final, 11.12.2002, Brussels.

---- (2003), *First report on the implementation of the Data Protection Directive (95/46/EC*), Brussels, 15.5.2003, COM(2003) 265 final.

---- (2004), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited communications or 'spam*', COM(2004) 28 final, 22.01.2004, Brussels.

---- (2004), *Questionnaire on the implementation of the Communication on unsolicited commercial communications or 'spam' (COM (2004) 28), 'the Communication'),* October, Brussels.

---- (2004), *Commission Staff Working Document Annex to the Proposal for a Regulation to the European Parliament and to the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas: Extended Impact Assessment*, SEC(2004) 1628, 28.12.2004, Brussels.

---- (2005), *Communication from the Commission: Compliance with the Charter of Fundamental Rights in Commission legislative proposals: Methodology for systematic and rigorous monitoring,* COM(2005) 172 final, 27.4.2005, Brussels.

---- (2005), *Communication from the Commission to the Council and the European Parliament. The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice*, COM(2005) 184 final, 10.5.2005, Brussels.

---- (2005), *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "i2010 – A European Information Society for growth and employment"*, COM(2005) 229 final, 1.6.2005, Brussels.

---- (2005), *Impact assessment guidelines*, SEC(2005) 791, 15 June, Brussels.

---- (2005), *Impact Assessment Annex to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*, Commission Staff Working Document, COM(2005) 475 final, 4.10.2005.

---- (2006), *Fact Sheet on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of judicial and police cooperation in criminal matters*, SCADPlus, updated 31.3.2006.

---- (2006), *Commission Working Document on the feasibility of an index of third-country nationals convicted in the European Union*, COM(2006) 359 final, 4.7.2006.

---- (2006), *Green Paper on detection technologies in the work of law enforcement, customs and other security authorities*, COM(2006) 474 final, 1.9.2006, Brussels.

---- (2007), *Communication to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, (COM(2007) 87 final*, 7.3.2007, Brussels.

---- (2007), *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs),* COM(2007) 228 final, 2.5.2007, Brussels.

---- (2007), *Information and Communication Technologies (ICT) – A Theme for research and development under the specific programme "Cooperation" implementing the Seventh Framework Programme (2007-2013) of the European Community for research, technological development and demonstration activities*, *Work programme 2007-08*, C(2007)2460 of 11 June.

---- (2007), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the outcome of the Review of the EU regulatory framework for electronic communications networks and services in accordance with Directive 2002/21/EC and Summary of the 2007 Reform Proposals*, COM(2007)696 rev1.

---- (2007), *Commission Staff Working Document Accompanying document to the Communication from The Commission to the European Parliament and the Council on Public-Private Dialogue in Security research and Innovation: Impact Assessment,* SEC(2007) 1138, 11.9.2007, Brussels.

---- (2007), *Results of the public online consultation on future Radio Frequency Identification Technology Policy "The RFID Revolution: Your voice on the challenges, opportunities and threats" accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework,* COM(2007)zzz final, SEC(2007)312, Brussels.

---- (2007), *Proposal for a Council Framework Decision on the Use of a Passenger Name Record (PNR) for law enforcement purposes*, presented on November 6.

---- (2007), *Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation*, COM(2007) 698 final, 13.11.2007, Brussels.

---- (2007), *Accompanying document to the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Summary of the Impact Assessment*, Commission Staff Working Document, SEC(2007) 1422. Brussels.

---- (2008), *Communication from the Commission to the European Parliament and to the Council On an entry/exit system at the external borders of the European Union, facilitating of border crossing for bona fide travelers, and an electronic travel authorisation system*, COM(2008)final, Brussels.

---- (2008), *Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the*

Regions "Preparing the next steps in border management in the European Union": Impact Assessment, Commission Staff Working Document SEC(2008) 153, 13.2.2008, Brussels.

---- (2008), *Agenda for the 7th meeting of the i2010 High Level Group,* 27 June, Brussels.

European Council (2005), *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union,* Official Journal of the European Union, C 53, 3.3.2005, pp. 1-14.

European Data Protection Authorities (2007), Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement, Cyprus, 11 May.

---- (2007), *Declaration adopted in Cyprus on 11 May 2007*, Cyprus, 11 May.

European Data Protection Supervisor (EDPS) (2005), *The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents,* Policy Paper, 18 March, Brussels.

---- (2006), *Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final*), OJ C 116, 17.5.2006.

---- (2006), *Communication from the Commission to the Council and the European Parliament: Evaluation of EU policies on Freedom, Security and Justice,* COM(2006) 332 final, 28.6.2006, Brussels.

---- (2006), *Second opinion on the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters,* 29 November, Brussels.

---- (2006), *Inventory 2007,* December, Brussels.

---- (2007), *Annual Report 2006*, Office for Official Publications of the European Communities, Luxembourg.

---- (2007), *Opinion on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with the view of adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime*, 4 April.

---- (2007), *Opinion on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, 25 July, Brussels.

---- (2007) *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007)96*, 20 December, Brussels.

---- (2008), *Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 26 March, Brussels.

---- (2008), *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning*

the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 10 April, Brussels.

---- (2008), *Opinion of the European Data Protection Supervisor on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism, and cross border crime,* Official Journal of the European Union, C 89, 10.4.2008, pp. 1-7.

---- (2008) *The EDPS and EU Research and Technological Development,* Policy Paper, 28 April, Brussels.

---- (2008), *Annual Report 2007,* Brussels.

European Economic and Social Committee (2005), *Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC* [(COM(2005) 438 final — 2005/0182 (COD)], Official Journal C 069 , 21/03/2006, pp. 16-21.

European Group on Ethics in Science and New Technologies (2005), *Ethical aspects of ICT implants in the human body*, Rapporteurs: Stefano Rodotà and Rafael Capurro, adopted on 16 March.

European Parliament (2007), *European Parliament resolution of 21 June 2007 on consumer confidence in the digital environment (2006/2048(INI)),* 21 June, Strasbourg.

---- (2008), *Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs, for the Committee on the Internal Market and Consumer Protection on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation(EC) No 2006/2004 on consumer protection cooperation*, Rapporteur: Alexander Alvaro, 18.4.2008.

FINKE, Barbara (2007), "Civil society participation in EU Governance", *Living Reviews in European Gov*ernance, No. 2, retrieved from: http://www.livingreviews.org/lreg-2007-2.

FLAHERTY, David H. (1989), *Protecting Privacy In Surveillance Societies,* Chapel Hill: University of North Carolina Press.

FRATTINI, Franco (2004), *Data protection in the area of Justice, Freedom and Security*, Speech for Meeting with the Joint Supervisory Authorities under the Third Pillar, SPEECH/04/549, Brussels, 21 December.

FREEDLAND, Mark (1999), *Data protection and employment in the European Union: An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and its Member States,* Oxford, for the European Commission, Directorate-General for Employment and Social Affairs.

GALLUP Organization (2008), *Data Protection in the European Union: Citizens' perceptions*, Analytical Report, Flash Eurobarometer 225, February.

GEYER, Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice,* Research Paper No. 9, CEPS, Brussels, May.

GONZÁLEZ FUSTER, Gloria and Pieter PAEPE (2008), "Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects" in GUILD, Elspeth and Florian GEYER

(eds.), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate, pp. 129-150.

GUERRERO PICÓ (2005), "El derecho fundamental a la protección de datos de carácter personal en la Constitución Europea", Revista de Derecho Comunitario Europeo, n° 4, Julio-Diciembre, pp. 293-332.

GUTWIRTH, Serge (2002), *Privacy and the information age,* Lanham, Rowman & Littlefield Publishers.

HAYES, Ben (2006), *Arming Big Brother: The EU's Security Research Programme*, TNI Briefing Series, No 2006/1, Transnational Institute: Amsterdam, April.

HEISENBERG, Dorothee (2005), *Negotiating Privacy: the European Union, the United States and Personal Data Protection*, London: Lynne Rienner Publisher.

HERVEY, Tamara (2006), *The European Union and the Governance of Health Care*, Paper presented at the annual meeting of the Law and Society, J.W. Marriott Resort, Las Vegas, October.

HIJMANS, Hielke (2006), "The European Data Protection Supervior: The Institutions of the EC Controlled by an Independent Authority", *Common Market Law Review,* 43, pp. 1313-1342.

HOGAN & HARTSON and ANALYSYS (2006), *Preparing the Next Steps in Regulation of Electronic Communications - A contribution to the review of the electronic communications regulatory framework*, Final Report, Study for the European Commission, July.

House Of Lords, European Union Committee (2005), *European Union: Fifth Report*, European Union Committee Publications, Session 2004-2005, 22 February.

---- (2007), *Schengen Information System II (SIS II), Report with evidence,* 9th Report of Session 2006-2007, HL Paper 49, The Stationery Office, London, 2 March.

---- (2008), *The Treaty of Lisbon: An Impact Assessment,* 10th Report of Session 2007-2008, HL Paper 62, The Stationery Office, London, 13 March.

House Of Lords European Committee (2007), *Prüm: an effective weapon against terrorism and crime?*, Report with Evidence, HL Paper 90, 18th Report of Session 2006-07, The Stationary Office Limited: London, 9 May.

House Of Lords / House Of Commons Joint Committee On Human Rights, (2008), *Data Protection and Human Rights*, Fourteenth Report of Session 2007-08. HL Paper 72, HC 132, London: The Stationery Office Limited, 14 March.

HUSTINX, Peter J. (2005), "Data Protection in the European Union", *P&I,* pp. 62-65.

HUSTINX, Peter (2008), *Strategic challenges for data protection in Europe*, speech delivered at the 9th Data Protection Conference, 6 May, Berlin.

Impact Assessment Board of the EC (2007), *Opinion on the Impact Assessment on the Communication on the creation of an entry/exit system at the external borders of the EU and on facilitating border crossing for bona fide travellers*, 4 December, Brussels.

International Working Group on Data Protection in Telecommunications (2008), *Report and Guidance on Privacy in Social Networks Services*, *'Rome memorandum'*, 43rd Meeting, 3-4 March 2008, Rome.

Joint Committee Meeting at the initiative of the European Parliament and the Assembleia da República of Portugal (2007), *The future of the EU as an area of Freedom, Security and Justice: Replies to a questionnaire to National Parliaments*, European Parliament, Brussels.

KORFF, Douwe (1998), *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*, Study Contract ETD/97/B5-9500/78, Commission of the European Communities, Final Report, October, Brussels.

---- (2005), *Data Protection Laws in the European Union*, Richard Hagle, Belgium: Federation of European and Interactive Marketing, 2nd Edition.

KUNER, Christopher (2003), *European Data Privacy Law and Online Business*, New York: Oxford University Press.

LEENES, Ronald, Jan SCHALLABÖCK and Marit HANSEN (2008), *PRIME White Paper*, Final version, 15 May.

LENOBLE, J. and M. MAESSCHALCK (2006), *Beyond Neo-institutionalist and Pragmatist Approaches to Governance*, Working Paper Series REFGOV-SGI/TNU-1, Reflexive Governance in the Public Interest (REFGOV).

LINDEN CONSULTING, Inc. (2007), Privacy Impact Assessments: International Study of the Application and Effects, prepared for Information Commissioner's Office (United Kingdom), Loughborough University, October.

MARTENCZUK, Bernd and Servaas VAN THIEL (eds), *Justice, Liberty, Security: New challenges for EU external relations,* VUB Press: Brussels.

MEEK, Colin (2008), *Consumer requirements for RFID standardisation,* Intertek Research and Performance Testing Report, commissioned by the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC).

MEUWESE, Anne (2008), *Impact assessment in EU law making*, E.M. Meijers.

MURAKAMI WOOD, David and Kirstie BALL (eds.) (2006), *A Report on the Surveillance Society, for the Information Commissioner by the Surveillance Studies Network,* September.

NEWMAN Abraham (2008), "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", *International Organization,* 62, Winter, pp. 103-30.

Office of Foreign Assets Control, US Department of the Treasury (2007), *Publication of US/EU Exchange of Letters and Terrorist Finance Tracking Program Representations of the United States Department of the Treasury*, Federal Register, Vol. 72, No. 204, 23 October.

PEARCE, Graham, and Nicholas PLATTEN (1998), "Achieving Personal Data Protection in the European Union", *Journal of Common Market Studies,* Volume 36, No. 4, Blackwell Publishers, December, pp. 529-547.

POULLET, Yves (2006), "The Directive 95/46/EC: Ten years after", *Computer Law & Security Report*, 22, pp. 206-217.

POULLET, Yves and Jean-Marc DINANT (2004), *L'autodétermination informationnelle à l'ère d'Internet : Eléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif (T-PD),* Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, Strasbourg, 18 novembre.

POULLET, Yves and Serge GUTWIRTH, “The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of ‘reflexive governance’?”, forthcoming.

PRESIDENCY OF THE COUNCIL (2001), Note 6316/2/01 JAI 13, From the Presidency to Article 36 Committee, “Subject: Draft Resolution on the personal data protection rules in instruments under the third pillar of the European Union”, 12 April, Brussels.

RAAB, Charles et al. (1998), *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data: Test of the Method on Several Categories of Transfer*, University of Edinburgh, European Commission Tender No. XV/97/18D, September.

RAMBØLL MANAGEMENT (2005), *Economic Evaluation of the Data Protection Directive,* Final Report, May, Copenhagen.

REGAN, Priscilla M., “American Business and the European Data Protection Directive: Lobbying Strategies and Tactics” in BENNET, Colin J., and Rebecca GRANT (eds.) (1999), *Visions of privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, pp. 199-216.

RESEAU UE D’EXPERTS INDEPENDANTS SUR LES DROITS FONDAMENTAUX (CFR-CDF) (2003), *L’équilibre entre liberté et sécurité dans les réponses de l’Union Européenne et de ses Etats membres à la menace terroriste,* Observation thématique, 31 mars.

RODOTÀ, Stefano (2006), “La conservación de los datos de tráfico en las comunicaciones electrónicas”, *Revista de los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya (UOC) (IDP*), N.°3.

RUIZ MIGUEL, Carlos (2003), “El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico”, *Revista de Derecho Comunitario Europeo*, Año 7, Número. 14, Enero-Abril, pp. 7-43.

SABEL, Charles F., and Jonathan ZEITLIN (2007), *Learning from difference: the New Architecture of Experimentalist Governance in the European Union*, European Governance Papers (EUROGOV), No. C-07-02.

SMISMANS, Stijn (2003), “European Civil Society: Shaped by Discourses and Institutional Interests”, *European Law Journal,* Vol. 9, No. 4, September, pp. 482-504.

---- (2007), “How political theory could deal with the role of civil society organisations in European governance: reflexive deliberative polyarchy”, in RUZZA, Carlo and Vincent DELLA SALA (eds.), *Governance and Civil Society in the European Union: Normative Perspective*, Manchester: Manchester University Press.

SMISMANS, Stijn (ed.) (2006), *Civil Society and Legitimate European Governance*, Cheltenham: Edward Elgar.

Standing Committee Of Experts On International Immigration, Refugee And Criminal Law (Commissie Meijers) (2007), *Note to Mr. Jacques Verraes on the proposal to give law enforcement authorities access to Eurodac*, 6 November.

Standing Committee Of Experts On International Immigration, Refugee And Criminal Law (Commissie Meijers) (2008), *Note to the Civil Liberties, Justice and Home Affairs Committee of the European Parliament regarding Views on the Commission report on the evaluation and future developmnet of the FRONTEX agency (COM(2008) 67 final)*, 4 April.

TONER, Helen (2006), “Impact assessments and fundamental rights protection in EU law”, *European Law Review,* 31, June, pp. 316-341.

TREACY, Bridget (2008), “Enforcement: EU Data Protection”*, Privacy & Security Law*, Volume 7, Number 12, 24 March, pp. 439-442.

TREIB, Oliver, Holger BÄHR and Gerda FALKNER (2005), *Modes of Governance: A Note Towards Conceptual Clarification*, European Governance Papers (EUROGOV) No. N-05-02.

TRANSATLANTIC CONSUMER DIALOGUE (TACD) (2007), *2006 Recommendations report and European Commission Services' Responses,* May.

WIK-CONSULT and RAND EUROPE (2008) *Comparison of Privacy and Trust Policies in the Area of Electronic Communications*, Final Report, Study for the European Commission, January.

Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data And Working Party On Police And Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007,* WP145, WPPJ 01:07, December.

6. 2 Legislation and case law

Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, C 364, 18.12.2000, pp. 1-22.

Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 303, 14.12.2007, pp. 1-16.

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour principles and related frequently asked questions issued by the US Department of Commerce (2006/520/EC), Official Journal of the European Communities, L 215, 25.8.2000, pp. 7-47.

Commission Decision of 11 May 2005 on the renewal of the mandate of the European Group on Ethics in Science and New Technologies (2005/383/EC), Official Journal of the European Union, L 127, 20.5.2005, pp. 17-19.

Commission Decision 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 (2004/535/EC), Official Journal of the European Union, 6.7.2004, L 235, pp. 11-22.

Commission Decision of 15 March 2006 on setting up a high level expert group to advise the European Commission on the implementation and the development of the i2010 strategy (2006/215/EC), Official Journal of the European Union, L 80, 17.3.2006, pp. 74-75.

Commission Decision of 28 June 2007 setting up the Expert Group on Radio Frequency Identification (2007/467/EC), Official Journal of the European Union, L 176, 6.7.2007, pp. 25-30.

Commission Decision of 25 March 2008 setting up the ‘Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime’ group of experts, (2008/324/EC), Official Journal of the European Union, L 111, 23.4.2008, pp. 11-14.

Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, Prüm, 27 May 2005.

Council Act 95/C316/02 of 26 July 1996 drawing up the Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes, OJ C 316 of 27 November 1995, pp. 33-42.

Council Act of 26 July 1995 drawing up the Convention based on Article K.3d of the Treaty on European Union on the establishment of a European Police Office (Europol Convention), OJ C 316 of 27.11.1995, p. 1.

Council Decision of 28 February 2008 implementing Regulation (EC) No 168/2007 as regards the adoption of a Multi-annual Framework for the European Union Agency for Fundamental Rights for 2007-2012, Official Journal of the European Union, OJ L 63, 7.3.2008, pp. 14–15

Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention), OJ L 271 of 24.10.2000, pp. 1-3.

Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 6.3.2002, pp. 1-13.

Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, Official Journal of the European Union, L 183, 20.5.2004, pp. 83-85.

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Official Journal of the European Union, L 205, 7.8.2007, pp. 63-81.

Council of Europe (1950), The European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4 November.

---- (1981), Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series, no. 108 of 28 January.

---- (2001), Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, Strasbourg, 8.XI.2001.

Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 62, 5.3.2002, p. 1–5.

Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, Official Journal of the European Union, L 53, 22.2.2007, p. 1–14.

Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal, L 281, 23.11.1995, pp. 31-50.

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, Official Journal, L 24, 30.1.1998, pp. 1–8.

Directive 99/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, Official Journal L 91, 7.4.1999, pp. 10-28.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal of the European Communities, L 108, 24.4.2002, p. 33-50.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, known as the 'e-Privacy Directive'), Official Journal, L 201,pp. 37-47, 31.7.2002.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Communities, L 105, pp. 54-63, 13.4.2006.

Judgement of the Court of 20 May 2003, *Rechnungshof* (C-465/00) *v Österreichischer Rundfunk and others and Christa Neukomm* (C-138/01) *and Joseph Lauermann* (C-139/01) *v Österreichischer Rundfunk*. Joined Cases C-465/00, C-138/01 and C-139/01, European Court reports 2003, p. I-04989.

Judgment of the Court of 6 November 2003, *Bodil Lindqvist*, C-101/01, European Court reports 2003, p. I-12971.

Judgement of the Court (Grand Chamber) of 30 May 2006, *European Parliament v Council of the European Union*, Joined Cases C-317/04 and C-318/04 (2006/C 178/02), Official Journal of the European Union, C 178, 29.7.2006, p. 1–2.

Organization for Economic Co-operation and Development (OECD) (2007), *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*, adopted by the OECD Council on 12 June.

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, Official Journal of the European Communities, L 8, 12.1.2001, pp. 1- 22.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Official Journal L 77, 13.3.2004, p. 1–11.

Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, Official Journal of the European Union, L 381, 28.12.2006, pp. 1-3.

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Official Journal of the European Union, L 381, 28.12.2006, pp. 4-22.

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, Official Journal L 239, 22.9.2000, p. 19–62.

Treaty establishing a Constitution for Europe, Official Journal of the European Union, 2004/C 310/01, pp. 1-474.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ 2007/C 306 Vol. 50.

United Nations (1990), Guidelines concerning computerized personal data files, adopted by the General Assembly on 14 December.

9. List of abbreviations

AEDH	European Association for Human Rights
ALCEI	Associazione per la Libertà nella Comunicazione Elettronica Interattiva
ANEC	European Association for the Co-ordination of Consumer Representation in Standardisation
BEUC	European Consumer's Organisation
BSA	Business Software Alliance
CIP	Competitiveness and Innovation Programme
CIS	Customs Information System
DG	Directorate-General
EC	European Commission
ECJ	European Court of Justice
ECLN	European Civil Liberties Network
ECSC	European Coal and Steel Community
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights Initiative
EESC	European Economic and Social Committee
EFF	Electronic Frontier Foundation
EGE	European Group on Ethics in Science and New Technologies
ENISA	European Network and Information Security Agency
EP	European Parliament
EPIC	Electronic Privacy Information Center
EU	European Union
EURATOM	European Atomic Energy Community
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
ETP	European Technology Platform
FEDMA	Federation of European Direct and Interactive Marketing
FIDH	International Federation for Human Rights
FIDIS	Future of Identity in the Information Society
FP7	7th Framework Programme
GoP	Group of Personalities
IAB	Interactive Advertising Bureau
ICT	Information and Communication Technologies
IST	Information Society Technologies
ISTAG	Information Society Technologies Advisory Group
INFSO	Information Society and Media
JHA	Justice and Home Affairs
NGO	Non Governmental Organisation
PETs	Privacy Enhancing Technologies
PI	Privacy International
PIAs	Privacy Impact Assessments
PRIME	Privacy and Identity Management for Europe
PRISE	Privacy Enhancing Shaping of Security Research and Technology
PSP	Policy Support Programme
ORG	Open Rights Group
R&D	Research and Development
SIS	Schengen Information System
SIS II	Second generation of the Schengen Information System
TACD	Transatlantic Consumer Dialogue

UK	United Kingdom
US	United States
VIBE	Verein für Internet-Benutzer
VIS	Visa Information System