The contribution of the Article 29 working party to the construction of a harmonised European data protection system

GUTWIRTH, Serge; Poullet, Yves

Published in:
Human rights in the web of governance

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

B. *DATA PROTECTION IN THE EUROPEAN UNION*

THE CONTRIBUTION OF THE ARTICLE 29 WORKING PARTY TO THE CONSTRUCTION OF A HARMONISED EUROPEAN DATA PROTECTION SYSTEM : AN ILLUSTRATION OF 'REFLEXIVE GOVERNANCE'?

BY

YVES POULLET

AND

SERGE GUTWIRTH

I. – Introduction (1)

To our knowledge, the establishment by Art. 29 of the Data Protection Directive (2) of an advisory and independent 'Working Party on the Protection of Individuals with regards to the Processing of Personal Data' (further referred to as : Art. 29 W.P.) is a unique event within the European institutional landscape. The Art. 29 W.P., which brings together representatives of the different national supervisory Data Protection Authorities, is a body responsible for giving advice and making recommendations to the European institutions on specific data protection issues. It works closely with the Commission. At European level, no similar institution has

(1) The main findings of this article were presented at a seminar held in Brussels the 26th of May, 2006 in the context of the Integrated Project : 'Reflexive Governance in the Public Interest' supported by the 6th Framework Programme of the EU Commission and coordinated by Prof. O. DE SCHUTTER (CDPR-UCL).

(2) Data Protection Directive : Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, OJ L 281, 23.11.1995, 31-50. This directive has been supplemented by data protection provisions in a number of more specific directives.

been established for example as regards consumer or environmental protection, although some national legislations do provide for supervisory bodies in these matters (3). To put it a little bit bluntly, it could be said that Art. 29 of the Data Protection Directive has officially installed a kind of 'privacy lobby group' at the heart of the European institutions. It must also be highlighted that the Working Party has a unique role to play not only in the process of ensuring the acquis of the European Data Protection, but also when it comes to progressively adapt the legislative framework and its effective application to the real needs of society in a changing context which still creates new privacy threats (4).

Taking the latter into account, as well as the recent debates about the draft EU Council Framework Decision on Data Protection in the Third Pillar (5) which intends to create a similar or integrated (6) institution as the Art. 29 W.P. (7), this chapter reflects upon the functioning of this institution, its impact on the Data Protection debates, its contribution to a better implementation and understanding of the Data Protection rules. At the same time, it examines how this institution might be viewed as a 'model' or 'tool'

(3) See the special issue of the *Utrecht Law Review* on *Supervision and Supervisiory Authorities*, Vol. 2/1, 2006 via www.utrechtlawreview.org, and Y. POULLET, 'L'autorité de contrôle : "vues" de Bruxelles', (1999) *Revue française d'administration publique*, 69-81.

(4) E.g. the global and interactive nature of the Internet has lead to an increase and intensification of our use of the Internet, and at once, of the generation of traces of this use, and thus also of possibilities and places where these traces might be processed. Also, the development of new ICT technologies – like RFID and biometrics – call for new debates and regulatory interventions. On these and many other subjects the Art. 29 W.P. issued opinions and published documents. All the documents, opinions, recommendations and reports of the Art. 29 W.P. are available at the Working Party's well organised website : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm. In the sequel of this contribution such documents, opinions, recommendations and reports will consequently be cited without reference.

(5) 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, COM(2005) 475 final of 4 October 2005 (available at http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0475en01.pdf).

(6) As regards the Art. 31 W.P. composition, the Draft Framework Decision foresees that each country is represented on a equal footing by a member of the Member state's Data Protection authority or authorities. Nowhere it is foreseen that these members have to be the same than those present within the Art. 29 W.P. and the Chairman elected by the Art. 31 W.P. might be different from the Art. 29 W.P. Chairman. Furthermore, the European Data Protection Supervisor, while he is full member of the Art. 29 W.P. has only a consultative role within the Art. 31 W.P. We will come back on the risks linked to these discrepancies between the compositions of the two W.P.'s as regards the consistency of the approaches followed in the two pillars.

(7) The list of competences granted to the Working Party settled by the Art. 31 of the Draft Decision is a copy of the competences foreseen by the Art. 30 of the Directive 95/46 for the Art. 29 W.P.

for ensuring 'reflexive Governance'. Our approach will start with an institutional description of the role, tasks and competences of the Art. 29 W.P. In a second step, we will consider the strategies developed by the Art. 29 W.P. to accomplish its tasks, notably the alliances it has developed with other actors. On that point we will give particular attention to the setting-up of the European Data Protection Supervisor (EDPS) (8) and to the present debate about the Data Protection in the Third Pillar. Finally, in a third and a fourth step, we will scrutinise the priorities and main achievements of the Art. 29 W.P. activities. Finally, we will try to conclude on the significance of the project and work of this Working Party for the central question of this book, namely the relevance of the hypothesis of 'reflexive governance' and 'learning-based' governance for the devising of a European human rights policy.

II. – The Art. 29 Working Party : an Institutional Approach

A. – *Composition*

To start with, the Art. 29 W.P. must be sharply distinguished from the Committee established by Art. 31 of the Data Protection Directive, which has been established to assist the Commission. While the Committee created by Art. 31 is composed by official representatives of the Member States' Governments and has decision

(8) Article 286 of the EC Treaty [now Art. 16 TFEU] provides that the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data also apply to its institutions and bodies from 1 January 1999 on. This Article also provides for the establishment of an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and for the adoption of any other appropriate provisions. The European Parliament and the Council have enacted Regulation (EC) 45/2001 concerning 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. This Regulation establishes an independent supervisory authority, called the European Data Protection Supervisor (EDPS), responsible for monitoring the processing of personal data by the Community institutions and bodies. Besides, each institution has a Data Protection Officer who will cooperate with the EDPS and in particular notify him of certain sensitive data processing operations, such as those relating to health matters and evaluation of staff. The status of the EDPS and general conditions governing the performance of the Supervisor's duties were defined by Decision no 1247/2002/EC of 1 July 2002. By a decision of the European Parliament and of the Council of 22 December 2003, published in the Official Journal of 17 January 2004, Mr Peter Johan Hustinx has been appointed as the EDPS and Mr Joaquín Bayo Delgado as Assistant Supervisor for a period of five years further to a public call for candidates. See the EDPS website : http://www.edps.europa.eu.

making competences (9), the Art. 29 W.P. has exclusively advisory powers and must 'be completely independent in the performance' of its duties (10). The Art. 29 W.P. is composed of representatives from the different independent supervisory authorities existing in the Member States (11). Taking into account that the number of Member States has suddenly increased from 15 to 27, and that the European Data Protection Supervisor has also been added with observer status, it is not obvious that the working procedure will not be subject to modification in the next future in order to maintain the present efficiency. Regular meetings (12) are organised in Brussels, including the annual conference of the European Data Protection Commissioners and the yearly International Conference of Data Protection Commissioners. No permanent independent secretariat exists, since the European Commission ensures this task (13). The simple majority rule (each member being recognized one vote) applies when a formal vote is needed, but most opinions and documents are adopted by consensus. Finally, we have to pinpoint the role of the chairman elected by the members of the W.P. This Chairman plays a leading role in the work of the group, by fixing its priorities and by defining with the Commission's secretariat the agenda of meetings.

B. – *Competences*

Article 30 extensively describes the different competences of the Art. 29 W.P. :

'1. The Working Party shall :

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(9) To be more precise, the Commission submits to the Art. 31 Committee a draft containing the measures envisaged. The Art. 31 Committee delivers an opinion at the qualified majority calculated on the basis of the Art. 14(2) EC. If the Committee's opinion is negative, the decision is differed during three months and communicated to the EU Council, which must answer the Committee's opinion.

(10) Data Protection Directive, recital 65 of the Preamble and Article 29 (1) al. 2.

(11) The question of the representation of the different regional D.P.A. in federal States like Spain, Germany and perhaps tomorrow Belgium is solved on an *ad hoc* basis for each country by designation. The representative is then, according the formula used by the Article 29 (2) al. 2a Data Protection Directive, a 'joint representative'.

(12) More or less four times per year.

(13) 'The Working Party's secretariat shall be provided by the Commission' (Art. 29(5)).

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the Committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall 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.'

Our ambition is not to discuss all these powers and competences in detail, but we would like to underline the following features. Since 1996, more than 120 opinions, recommendations and resolutions on various and often important topics have been issued by the Art. 29 W.P. This demonstrates an intense activity, a fact that is further evidenced in the Working Party's published and broadly distributed annual report. But beyond that visible activity, and perhaps even more importantly, there are the informal exchanges permitted and stimulated by the mere existence of the Working Party as a forum where representatives of the national data protection authorities regularly meet. The existence of such a forum has contributed to a large extent to a progressive harmonisation in the interpretation of the Data Protection Directive, even if this harmonisation is still not achieved.

C. – *Harmonisation*

Both from a theoretical and a pragmatic perspective, the major concern of the W.P. 29 seems to be to contribute to this harmonisation. In 2004 the Working Party, broadening its objectives, the Working party decided not only to examine regularly the implementation of the directive and its difficulties (14), but also to issue certain recommendations concerning the modalities of implementation of the Data Protection Directive by the Data Controllers. A good example is the recommendation of the Working Party about the way the duty of information has to be achieved by Data Controllers in accordance to Articles 10 and 11 of the Data Protection Directive (15). The Working Party analysed the discrepancies between the practices in different Member States and made certain recommendations, introduced as follows :

> 'In order to ensure a more consistent approach to information requirements, the Commission included "*More harmonised information provisions*" as a specific action item (Action 6) of the work programme for a better implementation of the Data Protection Directive and called on the Article 29 Working party to co-operate in the search for a more uniform interpretation of Article 10 (16). In the view of establishing a common approach for a pragmatic solution which should give a practical added value for the implementation of the general principles of the Directive the Art 29 Working Party hold a first discussion on this topic during its meeting on 22 June 2004 and adopted the following conclusions (...).' (17)

Finally, it should be noted that under Art. 30 2 of the Data Protection Directive, the Working Party has the obligation to inform the Commission about divergences in national legislations or practices, when they are likely to affect the equivalence of the Data Protection within the Community. We will come back on that issue further in this contribution.

(14) The first report on the implementation of the Directive 95/46 has been published by the Commission in 2003. See on this point the report itself (...) and the opinion of the Art. 29 W.P. on this report. It should be noticed that each annual report issued by the Art. 29 W.P. contains a short summary of the main events which occurred in the different Member States in the Privacy field (new legislation, new case-law, initiatives of the national DPA). Finally we have to pinpoint that on certain precise topics (see e.g. the Art. 29 W.P. document on e-government privacy issues) the Art. 29 W.P. is proceeding to a systematic comparison of the different national situations.

(15) See Art. 29 W.P., Opinion on More Harmonised Information Provisions, Nov. 25, 2004, W.P. 100.

(16) Commission's first report on the implementation of the D.P. Directive, COM(2003) 265 final.

(17) See at : http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm.

D. – *Opinions, Recommendations and other Documents*

Another important task of the Art. 29 W.P. is the delivery of opinions. Art. 30 of the Data Protection Directive foresees such opinions; they are expressly mentioned as regards certain points like, for instance, the adequate character of the protection offered by certain third countries, the suggested amendments or new regulatory proposals submitted by the EU institutions in the field of Data Protection (18) and finally on European Privacy Codes of conduct (19). Beyond these explicitly listed cases, the Art. 29 W.P. can issue opinions and recommendations – but also 'Working Documents', 'Letters' and other documents (20) – on its own initiative on all matters and topics related to data protection (21). This point has to be underlined insofar it illustrates that the Art. 29 W.P.'s role is not limited to advise the Commission, but that can intervene and *de facto* intervenes very freely and broadly about any topic related to data protection (22) including on matters that are not covered by the Data Protection Directive like general questions or trans-pillar issues (23).

It is important to stress the fact that the opinions and recommendations delivered by the Art. 29 W.P. are automatically and always transmitted to the European Commission, the European Parliament and the Art. 31 Committee, even when they do not con-

(18) In this respect one might quote recent the opinion of the Art. 29 W.P. on the EU Commission proposal for a Directive about Data Retention and its opinion on the Draft EU Council Framework Decision on Data Protection in the Third Pillar.

(19) Under article 28, EU companies are encouraged to adopt sectoral and European wide Codes of conduct which be submitted to the approval of the Art. 29 W.P. as regards their compliance with the Directive requirements. To this date, only one code of conduct has been subject to such procedure. See the Art. 29 W.P. opinions on the FEDMA (European Association on Direct Marketing) code.

(20) The Working Party is free to choose the most appropriate form of its decision. If the delivery of opinions is the most frequently mode used for issuing the its decisions, recommendations are typically used for expressing the 'catchall' competence of the Working Party. In other circumstances, taking fully benefit of the flexibility left to it, the Working Party has also issued documents under other, more informal, formats such as 'Working Documents' as regards the discussion of certain new issues like RFID, genetic data (17/03/04) or electronic Government, 'Joint statements' or 'endorsement letters' in case of emergency when reactions to the actuality or to concrete cases are needed.

(21) Art. 30(2) of the Data Protection Directive.

(22) The wording used by the Directive is interesting when at point c) of the Art. 30.1 a competence of 'advising on legislation and measures affecting Data Protection' is granted. The text refers not only to legislative documents explicitly intended for amending the Directive but also to any other Community measures which might affect data protection directly or indirectly.

(23) We will come back on this extension of competences in the description of the W.P. strategy.

cern suggested amendments or new regulatory proposals (24). Moreover, in Art. 11 of its Rules of Procedure, the Working Party has committed itself to publish and forward *any of its documents* (except the minutes or draft documents classified as restricted) to these bodies even if the text of Art. 30 4 Data Protection Directive only requires it for the opinions and recommendations (25). Furthermore, the Directive foresees the European Commission's obligation to inform the Working Party about the follow-up given to its opinions or recommendations, and this follow-up report shall also be forwarded to the European Parliament and the Council. That illustrates the importance given to the Art. 29 W.P.'s opinions since its creation insofar it would be possible for the two other European institutions to require from the Commission another follow-up of the W.P.'s opinions, recommendations or suggestions.

According to Article 14 of its Rules of Procedure, all documents adopted by the Working Party must be reasoned. This provides the addressees a better understanding of the arguments and reasons of the positions taken, and eventually helps them to integrate or challenge these documents in their final decisions.

III. – The Article 29 Working Party : a Strategic Approach

Beyond the institutional framework and the figures, we would like to focus on the strategies the Art. 29 W.P. is developing in order to increase its visibility and the overall the impact of its action. From this perspective we will address different points. Firstly, we will focus upon the relationships and alliances the Working Party is establishing and developing with the other actors, institutional or not. Secondly, we will analyse how the Art. 29 W.P. makes its best efforts to extend its competence beyond the scope provided by the Data Protection Directive. Thirdly, we will discuss how the Working Party has made the visibility of its actions and policy a main strategic concern. Finally, we will consider the different ways the Working Party fosters and promotes a practical and

(24) See e.g. Art. 29 W.P., Opinion on the Draft Directive on Traffic Data Retention, W.P. 119 (23/01/06).

(25) One might recall that the Working Party is subject to the 'Transparency Principle' enacted by the EU Regulation on public access.

effective cooperation amongst the national Data Protection Authorities (the D.P.A.).

A. – *A Strategy of Alliances*

As regards this first point, we make a distinction between the relationships the Working party has developed or is developing, on the one hand, with the other EU institutions (like the European Commission, Parliament or Council of Ministers) and on the other, with stakeholders in the field of data protection and privacy, such as civil society associations (e.g. in the field of human rights and consumer protection), trade unions and business associations.

1. *Alliances with EU-actors*

Amongst the relevant EU institutional actors, the *European Commission* is certainly a crucial partner and player to be taken into account by the Art. 29 W.P. As we have said before, the Commission, and more precisely the 'Data Protection Unit' within the D.G. Justice, Freedom and Security, provides its secretariat (26). In other words, the Art. 29 W.P. does not possess its own secretariat, office or budget. As a result of this situation, it is not rare that the W.P.'s documents are prepared jointly by the Commission and certain members of the Working Party.

Indeed, the European Commission (27) is not only the first ally, but also the first enemy of the Working Party. The proximity of both institutions and the obligations of the European Commission to take into consideration the opinions expressed by the W.P. and, as indicated earlier, to inform the W.P. about the follow-up given to the its recommendations and/or opinions leads the European

(26) Since 2005 the 'Data Protection Unit' is part of the D.G. Justice, Freedom and Security (previously DG Justice and Home Affairs). Before that, the Unit was integrated in the DG Internal Market (Markt). This change is entirely understandable : in 1995 the Data Protection Directive was considered as an outcome of the EU single market policy. The extension of the EU competences after the treaty of Amsterdam and the transversal importance of data protection made this change obvious. The personality of the successive heads of units and their personal concerns about data protection issues might also explain the quality of the relationships between the two institutions.

(27) As we will discuss later, within the organisation of European Commission, certain issues, which might have an impact on the Data Protection, are entrusted to European Commission's organs and other DGs than the DG Justice, Freedom and Security. That situation might create competition, rivalry and discrepancies because, from the perspective of these other DGs the Art. W.P. 29 interventions can easily be perceived as intrusions in their competences.

Commission to develop good synergies with the Working Party. It is quite clear that the Commission and the Art. 29 W.P. have jointly developed their position with regard to important and sensitive questions, such as Data Protection in the Third Pillar, and that they have in numerous delicate events defended the same position. In other cases however, the European Commission proposals have been severely criticised by the Art. 29 W.P., notably as regards the Passenger Name Record (PNR) or the Safe Harbour issues, when the political agreement reached by the European Commission with the U.S. administration did not correspond with the point of view of the Art. 29 W.P. Another illustration is provided by the debate about the Traffic Data Retention Directive (28). On the other hand, we must highlight the full confidence and importance that the Commission grants to the Art. 29 W.P. as regards its endeavours with regards to the harmonisation and implementation of the Data Protection Directive. The most significant example of this good cooperation might be found in the attitude of the Commission after the First Report about the implementation of the Data Protection Directive (2003) (29). This report underlined serious divergences as regards the national interpretations of the Directive. Rather than launching procedures against certain States for incorrect implementation of the Directive, the Commission preferred to develop a 'cooperative approach' grounded on a close cooperation of the Art. 29 W.P. and the national D.P.A. to rectify the identified inconsistencies. Furthermore, the Commission has explicitly requested to the W.P. to associate as soon as possible the national D.P.A. of the candidate countries.

(28) See Art. 29 W.P., Opinion 4/2005 on the Proposal for a Directive on the retention of Data processed in connection with the Provision of Public Electronic Communications Services and Amending Directive 2002/58/EC : 'However, the circumstances justifying data retention, even through they are said based on the requests coming from the competent authorities in Member States, do not appear to be grounded on crystal-clear evidence. Accordingly the proposed terms do not appear convincing as yet'.

(29) First Report on the implementation of Data Protection Directive (95/46/EC), 2003 (http://ec.europa.eu/justice_home/fsj/privacy/lawreport/report_en.htm). See, particularly, the Action 1 : 'Discussions in the Article 29 Working Party and in the Article 31 Committee will enable certain issues affecting a large number of Member States to be tackled on a multilateral basis, it being understood that there can be no question of such discussions leading to a *de facto* amendment of the Directive. In addition to *ad hoc* discussions on specific issues, the Commission proposes that each group devotes one complete meeting to this subject in the course of 2003' ; and action 3 : 'The Commission welcomes the Working Party's contributions to achieving a more uniform application of the Directive. It wishes to recall the importance of transparency in this process and encourages the efforts the Working Party is currently undertaking further to enhance the transparency of its work'.

The *European Parliament* positions itself even more strongly as the defender of human rights in the EU, and more specifically of privacy and data protection. This obviously explains an increasing implicit alliance between the Art. 29 W.P. and the European Parliament. Recently, in two major debates – namely the debates on PNR (30) and Traffic Data (31) – they have adopted common positions, and the European Parliament referred explicitly to the Art. 29 W.P. opinions in support of its arguments in favour of privacy and data protection. Furthermore, specific hearings of the Art. 29 W.P. have been organised by the European Parliament Committee on Citizens' Freedom and Rights, Justice and Home Affairs (32). This concerns more particularly the Public Security issues like the ECHELON problem and the impact of certain measures proposed by the EU Council of Ministers, such as the Draft Framework Decision on Data Protection in the third Pillar. Here, the alliance between European Parliament and the Art. 29 W.P. might be considered as a way to challenge the leadership of the Council of the EU. The Art. 29 W.P. has not hesitated to openly criticise the position of the Council in its documents, evoking its fruitful cooperation with the Parliament (33).

Finally, we must evoke the relationship between the Art. 29 W.P. and the recently established and appointed *European Data*

(30) The debate is not yet finished insofar the European Court of Justice has annulled the European Decision on traffic data by a judgment of 30 May 2006 (Joined Cases C-317/04 and C-318/04 *Parliament/Council* [2006] ECR I-4721). See, on that decision, the Art. 29 W.P. Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States, W.P. 122, 14 June 2006. On these debates, see M.V. Perez Asinari and Y. Poullet, 'The airline Passenger data disclosure case and the EU-US debate', (2004) 20 *Computer Law and Security Report* 2, 98-116; M.V. Perez Asinari and Y. Poullet, '"Airline passengers" data : adoption of an adequacy decision by the European Commission. How will the story end ?', (2004) 20 *Computer Law and Security Report* 5, 370-376.

(31) See on this long debate, Art. 29 W.P., Opinion 4/2005 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 of 21.09.2005), W.P. 113 adopted on 21st October 2005.

(32) 'Furthermore, as it has been mentioned already, over time the relationship between the Working Party and the European Parliament has become closer, with the latter endorsing most of the opinions of the Working Party in its Resolutions on data protection matters. The Working Party believes this dialog and co-operation must be improved further as the European Parliament, representing the views and concerns of the European citizens, has always been very sensitive to the safeguarding and promotion of the fundamental right of data protection.' ; Art. 29 Working Paper 98, *Strategy Document*, 29 September 2004.

(33) 'The W.P. also notes with regret the lack of independent advice in the Council as regards D.P. issues' ; Art. 29 Working Paper No. 98, *Strategy Document* 29/09/04.

Protection Supervisor (EDPS), although this analysis is a little premature (34). Even if in its first Policy Paper published on its web site (35), the EDPS has explicitly asserted that he and the Art. 29 W.P. will not have to act as competitors (36), it is quite obvious that rivalries might develop (37) due to the fact that they are sharing common competences, particularly as regards their respective advisory tasks towards the EU institutions on legislation and measures affecting Data Protection (38). Definitely, admitting the presence of the EDPS as a full member

(34) The EDPS was established in February 2004.

(35) See http://www.edps.europa.eu/.

(36) 'The Article 29-Working Party and the EDPS should not act as competitors but should wherever possible be complementary to each other (...).The EDPS shall assume his responsibilities with due respect to the specific qualities of the Article 29-Working Party. More concrete, the EDPS shall at first profit from his central position in the institutional framework. As a permanent body based in Brussels, and advising to the Commission, the Council and the European Parliament, he can give quick and flexible reactions on proposals and can give opinions in areas where the Working Party does not have a formal role (like the third pillar) or no specific competences or interest. The EDPS shall cooperate, where appropriate, with the Article 29-Working Party. This cooperation must lead to a division of tasks, in which the EDPS can adequately fulfil the tasks imposed upon him by Regulation (EC) 45/2001 and in the near future possibly based on Article I-51 and Article II-68 of the Constitution. At the same time, the European legislator must benefit as much as possible from the experiences on the national level, put forward by the Article 29-Working Party.'; EDPS – European Data Protection Supervisor: The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents, Policy Paper, Brussels, 18 March 2005 at http://www.edps.europa.eu/publications/policy_papers/policy_paper_advisor_EN.pdf. It should be noted that the present EDPS, the former Dutch Data Protection Commissioner P. Hustinx, has previously been the Chairman of the Art. 29 W.P., what might facilitate greatly the relations between both instances.

(37) Recently, for example, both institutions have delivered their opinions separately as regards the Draft Council Framework decision on Data Protection and police and judicial cooperation in criminal matters. More recently, as regards the judgment of the European Court of Justice on the PNR decisions, both institutions have differently reacted. On the one hand the EDPS seemed to conclude in favour of the necessity and urgency to devise a new exhaustive legislative instrument pertaining to data protection outside the scope of the first pillar. On the other hand, for the Art. 29 W.P. the judgment of the ECJ again highlighted the problems and difficulties related to the artificial division of data protection issues between the pillars and, consequently, the Working Party concluded that there is an urgent need for a coherent 'transpillar' data protection framework. About this issue see F. DUMORTIER and Y. POULLET, 'La protection des données à l'heure de la division entre piliers', APDCAT-Conference, Barcelona, 5th of Oct. 2006, to be published in the proceedings of the Conference.

(38) Art. 41(2) of the Regulation on the processing of Personal data by Community Institutions grants the EDPS the competence for advising the EU Institutions on all matters concerning the Data Protection. The European Court of Justice has endorsed a broad interpretation of this competence (see European Parliament, C-318/04/ECJ). See on that point the W.P.'s point of view expressed in its 2004 Strategy Document: 'The European Union institutional legal framework has recently been completed by the appointment of the first European Data Protection Supervisor (EDPS) and close cooperation and co-ordination is crucial, mainly in the area of giving advise on new legislation that can have an influence in the protection of individuals' rights and freedoms with regard to the processing of personal data, given the respective advisory roles of both the Article 29 Working Party and the EDPS'.

within the Art. 29 W.P. might facilitate the dialogue, but still the fact remains that the permanence of the EDPS, the existence of its own secretariat, its presence at Brussels might give to the latter certain advantages and pushes the Art. 29 W.P. aside in the dialogue with the EU organs. Undoubtedly, new working methods will have to be found in order to increase the cooperation and to avoid separate views coming from these two advisory Data Protection bodies.

2. *Alliances with other Stakeholders*

As regards the other stakeholders, such as private business associations, civil liberties associations, trade unions or consumer protection organisations, no significant efforts to cooperate and get their support have yet been made by the Art. 29 W.P. This is not surprising insofar the same consideration applies to the different national Data Protection Authorities. This is deplorable insofar the openness of the debates would be advantageous for both parties: on the one hand the Art. 29 W.P. would gain a better knowledge of the arguments expressed by the different stakeholders, and on the other the latter would more easily and directly obtain access to the Art. 29 W.P. opinions and become more aware of its positions. The lack of cooperation can be easily understood in the light of the Working Party's limited organisational means and availabilities. However, it must be added that representatives of the different stakeholders are invited in the context of conferences organised on a yearly basis by the EU Data Protection Commissioners or of hearings organized by the European Commission.

B. – *Enlarging competences*

As we already stated, the advisory role of the Art. 29 W.P. is very broadly defined by the Data Protection Directive. It is quite clear that the Art. 29 W.P. has, notwithstanding criticisms, taken full benefit of this situation in order to significantly enlarge its tasks beyond the strict enumeration of the Data Protection Directive. As a result, the Working Party has not hesitated to intervene frequently on topics directly related to issues linked to the growth of the Internet and the electronic communications sector, which

have been the object of the specific Directive 2002/58/EC (39). The Art. 29 W.P. produced a lot of documents about the issues at stake in this specific Directive (40). The same remark applies to the matter of data protection in the third pillar, although this clearly falls outside of the scope of the Data Protection Directive. Since the creation of the Data Protection Joint Supervisory Authority under the Schengen Convention, the Art. 29 W.P. has also tried to develop a close cooperation with this specific Authority (41). Next to that, it is relevant to note the Working party's multiple interventions about the ECHELON case (42), the PNR issues, and the Draft Directive on the retention of traffic data (43).

The main argument – that we endorse – developed by the Article 29 W.P. for extending its role in matters clearly outside the scope of the Data Protection Directive (44) goes as follows : if the principles of data protection are deduced from a fundamental right, or even stronger, if they simply *are* a fundamental human right, then they have to apply in any sector where personal data are processed, and as the Art. 29 W.P. is co-responsible for the implementation of the Data Protection Directive which provides these principles with their broadest expression, it must be also in charge of ensuring their compliance in all sectors in order to guarantee the highest degree of protection and uniformity of interpretation in these sectors. The concern to foster a uniform and consistent data protection regime in all relevant sectors (45), including the public security sector (police and law enforcement authorities) although this falls outside the scope both of the Personal Data Directive and of the first pillar of the Treaty on the European Union (46), has been strongly recalled by the Art. 29 W.P. in the recent discussion about data protection in the third pillar (47).

(39) The Directive 2002/58 on Privacy in the electronic communication sector and the follow-up of this Directive has been entrusted to the D.G. INFOSOC.

(40) See e.g. the Opinion 5/2004 on unsolicited communications for marketing purposes.

(41) This Joint Supervisory Authority was established to supervise the implementation of the 1984 Schengen Convention in general, and in particular, the SIS. On this Convention and the Joint Supervisory Authority, see the recent thesis defended by S.B. KARANJA, *Schengen Information System and Border Control Co-operation : A Transparency and Proportionality Evaluation*, Univ. of Oslo, June 2006 (to be published). About SIS II, see the more recent Art. 29 W.P. Opinion 6/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM(2005) 236 final) and a Council Decision (COM(2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final).

(42) Recommendation 2/99 concerning the respect for privacy in the context of the interception of telecommunications, adopted on May 3rd, 1999 (W.P. 18, 5005 99/final). On ECHELON, see the remarkable study by D. YERNAULT, 'De la fiction à la réalité : ECHELON, le programme d'espionnage électronique global et la responsabilité des Etats en ce qui concern le respect de la Convention européenne des Droits de l'Homme', (2000) *Revue belge de droit international*, 136 ff.

(43) See, e.g., Art. 29 W.P. Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council 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, delivered on 25 March 2006.

(44) In its judgment of 30 May 2006 on Joined Caes C-371/04 and C-318/04 (note 853) the European Court of Justice quashes the Commission's adequacy decision taken under the Article 25 of the Personal Data Protection Directive (95/46/EC) as exceeding the competences of the Commission. The main argument developed by the Court lays down on the fact that the PNR processing in question has as main purpose a public security objective which is clearly outside of the scope of EC law (first pillar of the Treaty on the European Union) and thus needed another legal basis.

C. – *Increasing its Visibility?*

The Data Protection Directive imposes an obligation on the Art. 29 W.P. to draw up an annual public activity report. Next to this first and self-evident way to ensure the visibility of the main

(45) See 8th Annual Report of the Art. 29 W.P., Introduction of the Chairman : 'For the Working Party, the year 2004 was characterised by the lasting dramatic conflict between the multiple attempts of European and foreign governments to implement new instruments in their fight against terrorism on one side, and the need to defend data protection principles as an essential element of freedom and democracy on the other side. The measures proposed by the Council, by Member States and by the Commission are activities within both the third and the first pillar. The European Parliament, the Council and the Commission disagree on the legal basis and, consequently, on the procedure to follow. The Working Party is formally part of the first pillar and there is no equivalent body for giving advice in the third pillar. There is a considerable risk that data protection implications will not be fully taken into account. The Working Party hopes that the Commission and Council will react soon on the appeal addressed to them by the European Data Protection Conference in their Wroclaw Resolution of September 2004 and provide for a comprehensive and effective organisation'.

(46) In its judgment of 30 May 2006 on Joined Caes C-371/04 and C-318/04 (note 30), the European Court of Justice quashes the Commission's adequacy decision taken under the Article 25 of the Personal Data Protection Directive (95/46/EC) as exceeding the competences of the Commission. The main argument developed by the Court lays down on the fact that the PNR processing in question has as main purpose a public security objective which is clearly outside of the scope of EC law (first pillar of the Treaty on the European Union) and thus needed another legal basis.

(47) 'The very recent approval by the European Parliament of a Directive of the European Parliament and of the Council on the retention of communication data can be viewed in the same perspective. These developments require the adoption of a legal instrument to guarantee an effective protection of personal data within all the Member States of the European Union, based on common standards (...). The new Framework should not only respect the principles of Data Protection (...) It is important to guarantee a consistency (...).' EDPS, Opinion of 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 cooperation in criminal matters (COM(2005) 475 final), Dec. 19, 2005. See also, in the same sense, W.P. 29, Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement, W.P. 122.

trends and outcomes of its work, many other tools have been developed by the Art. 29 W.P. in order to increase the accessibility and awareness of its activities and strategies. A public and broadly accessible website has been launched, providing access to a multitude of useful downloadable documents and studies, as well as relevant links. This website is managed and operated by the European Commission and fully integrated in the website of the European Commission's DG Justice, Freedom and Security. In recent years, the Art. 29 W.P. and the Commission have jointly opened an online consultation forum on different specific issues (48). This way of collecting reflections of all stakeholders including academics and individuals is interesting because it is a way to remedy and compensate the lack of direct dialogue between the Art. 29 W.P. and the stakeholders already underlined above. During the last annual conference of the EU D.P.A.'s, a reorganisation of the public activities of the Art. 29 W.P. and EU D.P.A.'s has been advocated, focusing on the need to set up a much more systematic contact with the press (for instance through press conferences).

Another initiative taken by the Art. 29 W.P. has to be highlighted. Since a few years, the Art. 29 W.P. publishes a 'roadmap' or a 'yearly work programme' which enumerates its main goals. This document can be seen as a manifestation of a proactive approach, since such roadmap can be used as a benchmark by any interested party. It also allows an *a posteriori* evaluation of the Working Party's achievements against the background of its own stated goals (49).

D. – *Fostering Practical and Efficient Cooperation amongst National Data Protection Authorities*

It is quite obvious that the regular meetings between national D.P.A. representatives do create multiple opportunities not only for formal and less formal exchanges, but also for the development of

(48) See notably the on line consultations organised on topics like RFID technology, binding corporate rules, videosurveillance, etc. The W.P. does regret the lack of responses coming from the public in the context of these consultations. Perhaps, the way by which the information and opinions are treated would have to be more clear and submitted to rules guaranteeing the freedom of expression and the neutrality and independence as regards the treatment of these opinions expressed.

(49) 'In order to increase the transparency of the activities of the Working Party and its openness to the society, the Article 29 Working Party will continue publishing a yearly Work Programme. The Work Programme will constitute an outline of the intended tasks of the Working Party and a clear indication of its priorities for the next year' (*Strategy Document*, 2004, 3.9).

habits of cooperation and mutual understanding. The D.P.A. representatives are regularly asked to address each other a short overview of the current situation of the privacy and data protection debates in their respective countries (e.g. with regards to recent case-law, initiatives taken by the D.P.A., press releases, public regulatory initiatives, (...)). In order to tackle specific issues, specific working groups have been installed on midterm duration about Spam, Internet, e-government, bringing together the appropriate specialists of the respective D.P.A.'s.

In the context of the Transborder Data Flows (TBDF), criticisms have been expressed by companies established in more than one EU country. When sending their data to third countries or to recipients offering adequate protection, they confront a number of difficulties due to discrepancies in the implementation of the Directive by the Member States. Their concern was to be able to address their questions to a unique counter, which might intervene for their different establishments. The same problem might exist with TBDF when appropriate contractual provisions or Binding Corporate Rules (BCR) are submitted by such multinational companies to the Member States in accordance with Article 26 of the Data Protection Directive. Responding to this concern, but only at this stage for BCR, the Art. 29 W.P. has established the principle of the unique counter and defined certain criteria for the D.P.A. in charge of this analysis.

The same concern exists for the EU data subjects when they face privacy threats caused by the TBDF recipients. In the context of the 'Safe Harbour Principles', the Art. 29 W.P. has set up a D.P.A. Panel bringing together the different national D.P.A.'s in order to facilitate the data subjects' applications. The panel fulfils a double function : not only does it assist the data subjects, but it also provides for a kind of alternative dispute resolution mechanism (50). It might also intervene in problems linked with contractual TBDF provisions. Furthermore, a bi-annual workshop and an internal network have been established by the Art. 29 W.P. and the different national D.P.A., in order to stimulate and organise the exchange of information about TBDF cases and to handle trans-national cases.

(50) It seems that this initiative has not met a success at the time of writing (on this see the intermediary report on the implementation of the Safe Harbour Principles by J. Dhont, M.V. Perez-Asinari, Y. Poullet with the cooperation of J. Reidenberg and L. Bygrave published on the website of the Art. 29 W.P.).

IV. – Two main Achievements of the Article 29 Working Party

A. – *The Fundamental Right to Data Protection*

The first major result of the work done by the Art. 29 W.P. is the inclusion in the Charter of Fundamental Rights in the European Union (adopted in Nice in 2000 (51)) of a new constitutional fundamental right : the right to data protection. This right is enshrined in Article 8 of the Charter (52) :

> 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.'

This right to data protection must be clearly distinguished from the right to privacy (or 'to respect for the private and family life, the home and the communications') enunciated by article 7 of the Charter in exactly the same wording as the first paragraph of Article 8 of the European Convention on Human Rights (ECHR) adopted within the Council of Europe in 1950.

This important distinction (53) has been clearly suggested and pushed forward by the Art. 29 W.P. (54). The main idea behind this new right is to take into account a fundamental evolution of the case-law of the European Court of Human Rights in Strasbourg, which (sometimes) tends to considerably enlarge the interpretation

(51) OJ C 364/1, 18.12.2000. See also : Article 29 Data Protection Working Party, *Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights*, 7th September 1999, available at : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp26en.pdf.

(52) Even if, for the time being, the Charter is not legally binding, the principles it codifies should be taken into account under the three pillars of EU law. The Charter stresses the nature of privacy and data protection as fundamental rights within the European Union and individualises each one, underscoring the autonomous function of each. The Charter, which the Treaty establishing a Constitution for Europe signed on 29 October 2004 proposed to include as Part II, shall be referred to as a binding source of EU law by the Reform Treaty, which is expected to be signed before the end of 2007. See the Draft Treaty amending the Treaty on European Union and the Treaty establishing the European Community (Draft Reform Treaty) (CIG 1/07, 23 July 2007).

(53) The importance of this distinction has been extensively discussed in P. De Hert and S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', in E. Claes, A. Duff and S. Gutwirth (eds), *Privacy and the criminal law* (Antwerp/Oxford, Intersentia, 2006), 61-104.

(54) S. Rodota, then Chairman of the W.P., played a great role in the adoption of this article by the drafters of the EU Charter of Fundamental Rights.

of the article 8 of the ECHR and to go from a 'Privacy-intimacy' concept to a 'Privacy-self determination' concept defined as the right to make its own choices in the society whatever it might concern : sexual relationships, environmental risks, employment conditions, etc. (55).

Conversely, as regards the personal data, the new perspective entailed by the recognition of an autonomous fundamental right to the protection of personal data no longer focuses on the protection of sensitive data, but aims more broadly at compensating the powers that the processing of personal data provides to the data controller, by limiting the use of personal data and by increasing the right to transparency granted to each data subject. More concretely this shift implies that the complex question 'is this a privacy issue ?' – or put differently, 'is this processing of these personal data violating Art. 8(1) ECHR ?' – is replaced by a far more easy one : 'are personal data processed ?'. Once the answer to the latter is affirmative, data protection applies.

The recognition of a new constitutional right to data protection is welcome for a number of reasons. First, it brings the two poles of the double logic of Data Protection Directive into balance, namely on the one hand the establishment of an internal market (in this case the free movement of personal data) and on the other hand the protection of fundamental rights and freedoms of individuals : by recognizing a fundamental right to data protection, the Charter unequivocally adds emphasis to the often overshadowed fundamental rights dimension of the Directive. Also, data protection explicitly aims at the requirements of fair processing, consent or legitimacy, which are not at the core of privacy and cannot be satisfactorily met by the case law of the Strasbourg Court (56). Furthermore, the Charter extends the pro-

(55) See e.g. S. Gutwirth, *Privacy and the information age*, (Lanham/Boulder/New York/Oxford, Rowman & Littlefield Publ., 2002), p. 158; S. Gutwirth and P. De Hert, 'De seks is hard maar seks (dura sex sed sex). Het arrest K.A. en A.D. tegen België', (2005) 3 *Panopticon*, 6 ff. and P. De Hert and S. Gutwirth, 'Privacy, data protection and law enforcement', cited above.

(56) P. De Hert and S. Gutwirth, 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence', in IPTS, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs* (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, 111-162. See also : ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.

tection of personal data to private relations and the private sector (57).

Last but not least, there is no ground in the ECHR and the case-law of the European Court of Human Rights for a right to have compliance with (all) data protection rules controlled by an independent authority, as is foreseen by the last paragraph of the new provision (58). The latter underlines the central role played by the Data Protection authorities in ensuring a fair balance between the legitimate Data controllers' right to process data and the Data Subjects' right to control the use of their informational image. This clear assertion contributes to give to the D.P.A. and their EU cooperation within the Art. 29 W.P. a fundamental place.

B. – *Tools for Coping with Transborder Data Flows*

A second major contribution of the Article 29 W.P. is definitely that, despite an unclear formulation in the Data Protection Directive, it has devised a comprehensive and well articulated system of tools for evaluating and ensuring the 'adequate protection' requirement in respect of transborder data flows (59), even if the methodology put progressively in place seems to need revision due to new ICT features, particularly in the area of the global and interactive Internet. Indeed, as a general principle, Article 25 obliges the third country to offer an adequate protection. This requires a strict interpretation of the other provisions, specially the exceptions based on the specific quality of the flow (Art. 26(1)). In accordance with the methodology proposed by Working Paper 12, delivered by the Arti-

(57) See Y. POULLET, 'Pour une justification des articles 25 et 26 en matière de flux tranfrontières et de protection des données', in M. COOLS, C. ELIAERTS, S. GUTWIRTH, T. JORIS and B. SPRUYT (eds), *'Ceci n'est pas un juriste ... mais un ami', Liber Amicorum Bart De Schutter*, (Brussels, VUBPress, 2003), 278.

(58) Article 13 ECHR (right to an effective legal remedy) is not an independent right. The European Court refuses to consider issues under this provision, when no other right of the ECHR is at stake.

(59) A survey of national practices in this regard, reveals considerable differences in approach. In certain countries the assessment is made by the data controller himself (Luxembourg), and in others by the Data Protection Authority (e.g. France and Portugal). In others still, the task is fulfilled by the Ministry of Justice (e.g. Netherlands and Sweden). On that situation, see Technical Annex of the Analysis and impact study on the implementation of the Directive EC 95/46 in Members States Fifth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and third countries : Covering the year 2000, EUR-OP, 2002 – 2 v. – ISBN 92-894-3571-2 – No. catalogue 39-01-001-EN-C.

cle 29 W.P. (60), a double assessment is required, which is based, not only on the *content* of the protection afforded by the third country's 'regulatory' system in the broadest sense, but also upon the *effectiveness* of the principles so enacted. This Article 25 approach might be considered as a pragmatic and case by case solution, that averts the risk of any European 'imperialism'. Beyond this first solution, by adding 'adequate safeguards' (Article 26(2)), the protection must no longer be obtained by an external regulatory framework, such as foreseen by Article 25. Instead it can be secured either by agreements (61), concluded between the exporter and the importer, or by the internal decisions taken by the multinational company, i.e. the famous 'binding corporate rules' (62). By thus proposing a variety of solutions to the European companies, the European Union is trying to satisfactorily respond to the multiplicity of needs faced by data controllers in relation to transborder data flows.

Thus, progressively and with the help of the Art. 29 W.P., the Commission has developed a diversified framework (proposing diverse solutions : legislation, contracts and self-regulation) for addressing the multiple TBDF issues while at once complying with the World Trade Organisation's requirement of non-discrimination (63). The approach is thus very open (64) :

(60) Article 29 Data Protection Working Party, *Working Document : Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*, 24th July 1998, W.P. 12.

(61) According to the competences granted to the Commission by Art. 26(4) of the Data Protection Directive, the Commission has adopted several standard contractual clauses upon the proposal of the Art. 29 W.P. proposal : Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181/19, 4.7.2001); Commission Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, available on http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm; and more recently the Commission Decision C (2004)5271 of 27 December 2004 OJ L 385/74, 29.4.2004, amending the Decision 2001/497/EC of 15 June 2001 on alternative clauses.

(62) Working Document on Transfers of personal data to third countries : Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 03.06.2003, W.P. 74.

(63) This implies that the regulation imposed by a State may not interfere with possible choice for external countries to meet the requirements enacted. On this aspect, see M.V. PEREZ-ASINARI, 'The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?', *18th BILETA Conference : Controlling Information in the Online Environment*, 2003, London. From the same author, 'Is there any room for Privacy and data Protection within the WTO rules', (2002) 9 *Electronic Communications Law Review*, 249-280.

(64) About this approach, Y. POULLET, B. HAVELANGE and A. LEFEBVRE, *'Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard*

- Firstly, it forbids any *a priori* judgment based on purely formal criteria. The fact that a country has ratified the Convention No. 108 is not per se a guarantee that the country offers an adequate protection. A case by case approach is needed to fully take into account the characteristics of the flow to be analyzed and the protection *effectively* offered by the recipient.
- Secondly, this attitude at the same time avoids any EU imperialism as regards the way by which the protection should be ensured. Under the wordings of Articles 25(2) and 26(2) of the Data Protection Directive, any regulatory means, including contractual provisions, self-regulatory systems or even the technology itself, might be taken into consideration for ensuring an adequate protection. As regards the value of self-regulatory norms, we might quote the decision taken by the Commission in 2000 about the TBDF towards the United States (65) and the opinions of the Article 29 W.P. on 'Binding Corporate Rules' (BCR) (66).
- Thirdly, while the effectiveness of the protection can be ensured by a variety of regulatory methods, in any case it must at a minimum provide for a complaints mechanism and, if needed, for the intervention of an independent authority (although not necessarily a public one : it can also be a private procedure for the resolution of the dispute by alternative means). This authority must have the power to investigate and to impose dissuasive sanctions. But these conditions of effectiveness can be realised in the context of a self-regulatory system like a code of conduct. This focus on the effectiveness explains why recently, the Article 29 W.P. has considered that the adequacy offered by the US 'Safe Harbour Principles' can be questioned not because the self-regulatory nature of the protection afforded, but because of its lack of actual effectiveness (67).

du traitement de données à caractère personnel'. Rapport Final. Centre de Recherches Informatique et Droit, University of Namur, Belgium. European Commission, DG XV. December 1996.

(65) Commission Decision 2000/520/EC of 26.7.2000 – OJ L 215/7, 25.8.2000.

(66) Working Document on Transfers of personal data to third countries : Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 03.06.2003, W.P. 74.

(67) On that point, see the recent report prepared in the context of the Safe Harbour revision, J. Dhont, M.V. Perez-Asinari, Y. Poullet with the collaboration of J. Reidenberg and L. Bygrave, *Safe Harbour Decision Implementation Study*, at the request of the European Commission, published on the web site of the Commission : http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf.

V. – The Priorities of the Art. 29 Working Party

A. – *The Monitoring of the ICT Technologies and the Promotion of a Techno-Legal Approach*

Since the explosion of the Internet, due to the interactive nature of the network and its large capacity, new threats to privacy have surfaced. In order to face them, the Data Protection Authorities have developed a more proactive policy (68) vis-à-vis the development of the information and communication technologies, either by forbidding uses of technology which might jeopardise privacy (69), or promoting technologies that fulfil data protection requirements within the infrastructure of the information systems, or including such measures within the terminal equipment. All these initiatives underline the attention to be paid to the technical aspects, as well as to the positive or negative impact that the technological choices embedded in our terminals or designing the infrastructure might arise in relation to the protection legally afforded to data subjects.

The Commission, in its first report on the implementation of the Directive 95/46/CE, has broadly emphasised the positive role of so-called 'privacy enhancing technologies' (PETs) (70) that are increasingly being cited as data protection tools. These are conceived either as a back-up to self-regulatory approaches, such as P3P (71), or as a substitute for other forms of regulation, such as

(68) See the recent declaration of the Article 29 W.P. : 'New Technologies have a crucial role in promoting economic, social and human development but, at the same time, if not properly implemented, could cause adverse impacts in the framework of guarantees for fundamental rights and data protection, enshrined in European Law. For that reason, the impact of new technologies on privacy has always been a prominent issue of the Working Privacy Party, as common expertise and guidance is essential in that field. Since its very early documents, there has been an ongoing interest in the relationship between emerging technologies and data protection and the Working Party has always tried to provide advice on their privacy compliant design and implementation'.

(69) What we call a Privacy Invasive Technology (PIT) ... like cookies, spyware, invisible hyperlinks and so on.

(70) H. Burkert, 'Privacy Enhancing Technologies. Typology, Critique, Vision', in P. Agre and M. Rotenberg (eds), *Technology and Privacy* (MIT Press, Cambridge MA, 2001), 125-143; L. Lessig, *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999), 26 ff.; J. Reidenberg, 'Lex informatica; the Formulation of Information Policy through Technology', (1998) 76 *Texas Law Review*, 552-593; Y. Poullet, 'Technology and Law : from Challenge to Alliance', in U. Gasser (ed), *Information Quality Regulation : Foundations, Perspectives and Applications* (Nomos Verlagsgesselschaft, 2004). For a presentation of PETs, See the EPIC site : http://www.epic.org/privacy/tools.html.

(71) See J. Catlett, *Technical Standards and Privacy : An Open Letter to P3P Developers*, at http://www.junkbusters.com/standards.html.

for example, encryption (72). Such approaches may be applied to the technological infrastructure (e.g. the automatic blocking of connections to countries that fail to comply with data protection rules); to data controllers or to intermediaries (e.g. through the use of filters by special servers to block spam sent by certain types of enterprise); or to data subjects' terminals (e.g. through tools that either prevent the sending and receiving of cookies or negotiate with the data controller). Through a number of research projects, wherein sometimes the D.P.A. are involved, the Commission hopes to promote both the awareness of these solutions and the development of new tools.

While the effective of such tools is widely acknowledged (73), critics require to focus on the rules that these tools apply. These rules are often agreed by experts who are not sufficiently aware of data protection requirements or are more sensitive to the needs of their industry than to data subjects' interests. When the technologies concerned have to be applied by the data subjects themselves, the notion of user empowerment is often something of a myth. Leenes and Koops, who endorse the potential of these PETs to enforce data protection law, do however also draw the attention to their user-*un*friendliness in respect of their installation and use (74). Moreover, how can individuals take responsibility for their own protection when the consequences of their decisions are not clear and when they sometimes have no choice in the matter? For example, there are sites that refuse access to users who do not accept cookies. Negotiations via P3P may be insidiously bypassed by data controllers who offer to 'pay' for personal data (75). Moreover, industry is not really interested in implementing privacy-enhancing technol-

(72) On the various encryption protocols and anonymous proxy servers as well as anonymisation tools and the use of pseudonyms, see C.J. Bennett and C. Raab, *The Governance of Privacy* (Ashgate, London, 2003), 148 ff.

(73) See PISA (Privacy Incorporated Software Agent), project launched in the context of the EU 5th Framework Programme which is aiming to offer an EU alternative to the P3P approach by promoting the data subjects information and protection. On this comparison and other reflections, J. Borking and C. Raab, 'Laws, PETS and other Technologies for Privacy Protection', (2001) *JILT*, 1 ff. See also the EU PRIME project available on the portal: www.prime-project.eu.org. PRIME elaborates a framework to integrate all technical and non-technical aspects of privacy-enhancing IDM.

(74) R. Leenes and B.J. Koops, '"Code": Privacy's Death or Saviour?', (2005) 19 *International Review of Law, Computers & Technology* 3, 239-340.

(75) See, for example, the conclusions of the PISA project: 'Privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing ... rather than relying on legal protection and self-regulation' (dbs.cordis.lu/fep).

ogy. They see no (economic) reason to do it (76). As Dix notes (77), technology should not be seen as a panacea for privacy risks in cyberspace; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather, it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation, but a necessary additional tool. In other words, neither useful technology, nor law are sufficient. Stakeholder awareness, social norms and market rules are also relevant. To say it with Lessig, the full effectiveness of any regulation depends on the optimal mixture of all accessible means (78).

Beyond these different actions, Recommendation 1/99 of the Article 29 W.P. (79) concerning the threats to privacy caused by Internet, communications software and hardware, establishes the principle that such industry products should provide the necessary tools to comply with European data protection rules. This obligation, to see the data protection requirements enshrined in the development of information systems has been emphasised again in a recent recommendation about Radio Frequency technology (RFID) (80). Article 14 of Directive 2002/58/CE states that, where required, the Commission may adopt measures to ensure that the functioning of the terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is

(76) R. Leenes and B.J. Koops, cited above, 336-337.

(77) A. Dix, 'RFID technology – New challenges for Privacy', in G. Rasi (*a cura di*), *Innovazioni technologiche e privacy, Garante per la protezione dei dati personali* (2005), p. 75 ff. See on that point also, the Article 29 Working Party reflections in Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), W.P. 11, June 16, 1998.

(78) L. Lessig, 'Commentaries, The Law of the Horse: What Cyberlaw Might Teach?', (1999) 113 *Harvard Law Review*, 501-546. See also P. Ahonen, P. Alahuhta, B. Daskala, P. De Hert, S. Delaitre, M. Friedewald, S. Gutwirth, R. Lindner, I. Maghiros, A. Moscibroda, Y. Punie, M. Verlinden, W. Schreurs, E. Vildjiounaite and D. Wright, *Final Report. Safeguards in a world of Ambient Intelligence*, D. Wright (ed), Deliverable D4, August 2006, 127. Available http://swami.jrc.es/pages/documents/SWAMID4-final.pdf.

(79) Recommendation on invisible and Automatic Processing of Personal Data on the Internet performed by Software and Hardware. Feb. 23, 1999, W.P. 17.

(80) 'In this context, Working Party 29 wishes to emphasize that while the deployment of an RFID application is ultimately responsible for the personal data gathered through the application in question, manufactures of RFID technology and standardisation bodies are responsible for ensuring that data protection/privacy compliant RFID technology is available for those who deploy the technology. Mechanisms should be developed in order to ensure that such standards are widely followed in practical applications. In particular, RFID privacy compliant standards must be available to ensure that data controllers processing personal data through RFID technology have the necessary tools to implement the requirements contained in the Data Protection Directive. The Working Party therefore urges manufactures of RFID tags, readers and RFID applications as well as standardisation bodies to take the following recommendations into account.' (Opinion of the Article 29 W.P. – Opinion 19.01.2005, already quoted).

another, albeit admittedly subsidiary way, of protecting personal data from the risks of unlawful processing – risks that have been created by these new technologies options.

To become involved into the standardisation process is another concern of the Article 29 W.P (81). In 2004, at the 26th International Conference on privacy and personal data protection, held in Krakow, the final resolution emphasised the need for Data Protection Commissioners to work jointly with standardisation organisations to develop privacy related technical and organisational standards (82). The recent CEN and ISO standards on security and privacy (83) are certainly a first step in that direction. However, the Data Protection Authorities must play their part in the debate which is currently taking place among private standardisation bodies such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN) and the World Wide Web Consortium (W3C).

B. – *The Effectiveness of the Data Protection Legislation : How to Achieve It?*

On 25 November 2004, the Working Party adopted a declaration on enforcement which summarises the outcome of the discussions at the subgroup level and at the plenary, and announces joint enforcement actions for 2005-2006 based on criteria contained in this document. The concept of enforcement is broadly defined by the Working Party 'as any action leading to better compliance, including awareness raising activities and the development of guidance. In a narrower sense, enforcement means the undertaking of investigative actions, or even solely the imposition of sanctions' (84).

(81) See as regards this concern, the Article 29 Working Party Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardization in Europe, W.P. 57, May, 30, 2002.

(82) Whereas the International Conference wishes to support the development of an effective and universally accepted international privacy technology standard and make available to ISO its expertise for the development of such standard ... Final resolution of the 26 International Conference on Privacy and Personal Data Protection (Wroclaw, September, 14, 2004), Resolution on a draft ISO Privacy standards).

(83) The Security and Privacy Standards Technical Committee is P member in ISO/IEC JTC1/SC27 – Security Standards. For more details on the ISO action on that field, see the website : www.itsc.org.sg/tc/5th_term_compo/spstc.html. Read also, the CEN/ISSS secretariat Final Report. 'Initiatives on Privacy Standardisation in Europe', February 13, 2002, available at : http://ec.europa.eu/enterprise/ict/policy/standards/ipse_finalreport.pdf.

(84) Declaration of the Art. 29 W.P. on enforcement, adopted the 24th of November 2004, W.P. 101.

A first initiative, already mentioned, has been taken in the 'Opinion on more harmonised information provisions' (W.P. 100), adopted the same day and aiming at simplifying and harmonising the obligation of companies to inform the citizens about the processing of their personal data. In its Opinion the Article 29 W.P. stressed how important it is to establish a common approach for a pragmatic solution, which should give a practical added value for the implementation of the general principles of the Directive towards developing more harmonised information provisions. The Working Party endorsed the principle that a fair processing notice does not need to be contained in a single document. Instead – as long as the sum total meets legal requirements – there could be up to three layers of information provided to citizens. The main aim of these first actions is to increase the awareness of the citizens about their rights and at the same time of the data controllers about their duties (85).

A second initiative was the call for reinforcing the role of data protection officials appointed within the data controllers' organisations. 'A broader use of data protection officials as a substitute to notification duties, at least with regard to certain industry sectors and/or in respect of larger organisations including those in the public sector, would be useful in view of the positive findings reported by the Member States in which these data protection officials have been already introduced or have existed traditionally' (86). The main purpose is to introduce directly at the data controllers' level a prior verification of the compliance of their processing activities with the Personal Data Protection Directive requirements. In other words, the Data Protection Authorities are searching for 'allies' directly incorporated in the data controllers' organisations and to develop, through cooperation amongst these data protection offi-

(85) 'The Working Party is of the view that awareness raising activities, the provision of guidance and advice to both data subjects and data controllers, the promotion of codes of conduct, etc, are no doubt important means for achieving compliance. The data protection authorities agree that there can be a relationship between a low level of knowledge of their rights among data subjects and compliance. A better knowledge of rights can enhance data protection awareness in society.' About the importance of this awareness for a better implementation of the Data Protection legislation, see Y. POULLET, 'Mieux sensibiliser les personnes concernées – Les rendre acteurs de leur proper protection', Proceedings of the Prague Conference organised by the Council of Europe, published in *Droit de l'immatériel,* (May 2005) Revue Lamy, 47 ff.

(86) Art. 29 W.P. 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, adopted on 18 January 2005, W.P. 106.

cials appointed in the same sector of activities and exchanges of best practices regarding the appropriate implementation of the data protection rules.

Enforcement also means the possibility of detecting, investigating and sanctioning the lack of compliance with data protection requirements. On that point, the Art. 29 W.P. pleads not only for a reinforcement of the means of action of the national data protection authorities, but also for coordinated national efforts directed towards specific sector of activities. 'An EU wide, synchronised national enforcement action would entail co-ordinated national *ex officio* investigations taking place in a certain period of time, focused at similar national processing and based on questionnaires agreed at EU level (...). The aim of such synchronised actions will primarily be to analyse whether and how the rules are being complied with in the sector, and, if necessary, the issuing of further recommendations (...). The implementation of the recommendations issued after these investigations will be monitored and, if necessary, sanctions could be imposed according to national laws' (87).

Finally, the Art. 29 W.P. has decided to increase its cooperative efforts to support a more coherent and consistent implementation of the Data Protection Directive by launching a wide synchronised investigation on certain cases or sectors of activities. In its 2004 *Strategy Document* it has stated the following :

> 'Co-operation among data protection authorities is highly desirable, both in their daily operations and as part of the planning of joint actions, and must be a prominent component of any strategic plan or policy. Several instruments are now in place to foster practical and efficient co-operation among European data protection authorities and are current examples of this commitment :
>
> – The biannual workshop on complaints handling and its Internet Network for exchange of information and handling trans-national cases;
>
> – The regular and informal exchange of information among the different DPAs in the form of questions and answers relating to the law and practice in every Member State;
>
> – The recent setting up of an on-line IT experts network;
>
> – The provisions for joint work that can be found in the document on Binding Corporate Rules;
>
> – The work on simplification of the notification of personal data processing for companies established in several Member States;

(87) Declaration of the Art. 29 W.P. on enforcement, adopted on 25 November 2004, W.P. 101.

> – The meetings and the leadership of the group of the national authorities involved with the enforcement of Community measures relating to unsolicited commercial communications or "spam".
>
> Finally, there is a strong will on the part of all the Data Protection Authorities of the Working Party to promptly answer any question or to fulfil any request of co-operation received from any other such Authority of another Member State to the greatest extent possible within its powers and competences.' (88)

In March 2006 this resulted in the launching of a first EU-wide investigation about the data protection practices in the private Healthcare Insurance sector (89).

C. – *Privacy v. Security : A Challenge*

The Chairman's introduction to the Art. 29 W.P.'s 8th Report of 2004 outlines the Working Party's concerns about all the governmental initiatives taken within the EU or by third countries after the attacks of September 11th, 2001. He wrote :

> 'The year 2004 was characterised by the lasting dramatic conflict between the multiple attempts of European and foreign governments to implement new instruments in their fight against terrorism on one side and the need to defend data protection principles as an essential element of freedoms and democracy on the other side.' (90)

The balance between the two essential values is put at risk when measures limiting our liberties in the name of public security are multiplied. The Art. 29 W.P. has seized every available opportunity to reaffirm the principles derived from the case-law of the European Court of Human Rights, principles based upon its interpretation of the article 8(2) of the ECHR in order to fight against abusive surveillance. From that perspective one might quote the opinions delivered on the transfer of passenger data towards the US Customs and Border Protection (91), about the use of genetic data (92), about the proposal of the directive on traffic data retention (93).

(88) Art. 29 W.P., *Strategy document*, WP98, 29 September 2004, p 6. (at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp98_en.pdf.

(89) See above on the initiatives to increase the effectiveness of the Data Protection Directive's provisions.

(90) Art. 29 W.P., Eight Annual Report on the protection of individuals with regard of the Processing of personal Data within the European Union and in third countries, Year 2004, November 2005.

(91) Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, 30/09/04, W.P. 97.

(92) Working Document on Genetic Data, 17/03/04, W.P. 91.

(93) Art. 29 Working Party, Opinion 4/2005 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 of 21.09.2005), W.P. 113, adopted on 21st October 2005.

This concern of the Art. 29 W.P. has been sharpened and amplified by the fact that there is no comprehensive data protection regulatory framework in the third pillar and, hence, that no body, equivalent to the Art. 29 W.P. has been set up for giving advice in matters of criminal justice and police work. The present discussion on the adoption of the Framework Decision for data protection in the third pillar (94) and the creation of a new body having competences similar to those of the Art. 29 W.P., might solve the question, but it will perhaps be too late, as many of the legislative measures restricting our liberties will have already been taken. The fear that the two Working Parties might work independently and might thus develop divergent interpretations about the same principles has been underlined by the EDPS report, whose presence within the Third Pillar Working Party was foreseen only with a consultative role in the first draft of the Framework Decision. Together with the EDPS (95) and the Roure Report of the LIBE Committee of the European Parliament (96), we plead for a coherent approach between pillars and therefore in favour of the establishment of two working groups having the same composition (97).

Beyond the debate between public security and data protection, other increasing risks have been pointed at by the Art. 29 W.P. such as electronic surveillance linked to the development of the ICT tools able to unfairly collect data in order to control the data subjects' behaviour. The Art. 29 W.P. has issued a number of opinions

(94) 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, Brussels 4 October 2005, COM(2005) 475 final.

(95) The EDPS 'emphasises the importance of a consistent approach on matters of data protection that could be enhanced by promoting the communication between the existing Article 29 Working Party and the Working Party established by the present proposal for a Framework Decision. The EDPS recommends an amendment of Article 31 (2) of the proposal so as to also entitle the chairperson of the Article 29-Working Party to participate or be represented in meetings of the new Working Party' (Opinion of 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 cooperation in criminal matters (COM(2005) 475 final) (2006/C 47/12).

(96) European Parliament, Report on the proposal for a Council Framework Decision on the protection of personal data in the framework of police and judicial cooperation in criminal matters, Report presented by M Roure, 18 May 2006, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, COM(2005) 0475-C6-0436/2005-2005/0202 (CNS).

(97) The EDPS and the Roure Report suggest only slight modifications: the presence of the Art. 29 W.P.'s chairman and the EDPS right to vote. We take the view that the same composition might be easily justified insofar until now, at the national level, the national Data Protection Authorities are competent both for first pillar and third pillar matters.

about these surveillance technologies such as video-surveillance (98), surveillance at the workplace (99), the detection of illicit copies by copyright holders (100), etc. More recently, it has published a working paper about a range of e-government issues, particularly e-identity cards, governmental portals and websites, cross-administration networks and other topics. Based upon an analysis of recent national developments and a systematic comparison of regulatory approaches, this document illustrates how the increasing aggregation of data by administration through different new ICT tools endangers our liberties (101).

VI. – The Art. 29 Working Party: an Illustration of 'Reflexive Governance' in the Field of Human Rights?

A. – *The Art. 29 Working Party: a Peculiar but nonetheless major Player*

Against the background of the former descriptions and analyses there is no doubt that the 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' established by Art. 29 of the Data Protection Directive is becoming a major player in the data protection system that has been set up in the EU, even though its powers are advisory and thus limited and in spite of its unique and original character, being a sort of institutionalised pressure group and awareness raiser in the EU framework. The Working Party has developed into a crucial knot or cluster in the network of actors which are concerned with the concrete realisation and implementation of the rules that were devised to enforce the fundamental right to data protection in the EU and its Member States.

(98) Working Document on the Processing of Personal Data by means of Video Surveillance, 25 November 2002, W.P. 67 and Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11 February 2004, W.P. 89.

(99) Working document on the surveillance of electronic communications in the workplace, 29 May 2002, W.P. 62.

(100) Working document on data protection issues related to intellectual property rights, 18 January 2005, W.P. 104. This Working Document has been established after a public consultation organised by the Art. 29 W.P.

(101) Working document on E-Government, 8 May 2003, W.P. 73.

We think that we have been able to show this at will : the independent Art. 29 W.P. works very closely with the Commission and has an effective impact on the way the European data protection acquis is built up and data protection policies are devised, adapted and implemented; it collaborates with the European Parliament and the EDPS; the Working Party often takes the lead, sometimes prospectively, in exploring and detecting new data protection threats and vulnerabilities related to changing contexts and the development of new technologies and practices; it actively contributes to the harmonisation and approximation of the Data Protection Directive by regularly examining the implementation of the directive and the obstacles it faces and by issuing recommendations on that point to the national Data Protection Authorities; up to now the Working Party has not only been an extremely active, visible and transparent player issuing and making readily available (through its website) a vast number of opinions, recommendations and resolutions, but it has also provided a regular informal meeting place for the different national Data Protection Authorities; it has, moreover, not hesitated to broaden its action radius beyond the strict scope of the Data Protection Directive to matters such as data protection in the third pillar and the electronic communications sector; it has also, for example, promoted the explicit recognition of a fundamental right to data protection in the Charter of Fundamental Rights in the European Union; and it has played a crucial role in finding and elaborating diverse solutions for the problems caused by TBDF.

Referring to its composition and powers the Art. 29 W.P. takes an interesting position : it brings together representatives of the different national data protection supervisory bodies with their diverse national backgrounds and experiences, but it generally acts as a unity, by consensus, at the level of the EU. On the one hand this implies a lot of mediative activity, reciprocal interest and mutual learning, and on the other there is the strong constraint to take into account a common European perspective and to jointly articulate and construct visions upon the future of data protection in Europe. Moreover, the mere existence of a formal forum such as the Working Party evidently provides many occasions of informal contacts among the national data protection representatives, contributing to a large extent to progressive approximation and articulation of the different national interpretations and implementations of the Data Protection Directive. Next to this it is striking to see how the Working Party has imposed itself as an interlocutor impossible to circumvent and actor in issues relating to data protection, more particularly towards both the national and European levels of governance.

The former conclusions are certainly linked to a range of drivers of the work of the Art. 29 W.P. Firstly, it must be stressed that the Working Party deliberately opted for *working methods* in which transparency, openness, communication, consultation and dialogue are the key principles. Thanks to its rather exhaustive website, it can be said a bit trivially that the Working Party says what it does and does what it says as regards its strategy, its positions and the outcomes of its work, and that all this is open to internal and external discussion. On the other hand, there is still a long way to go as regards the participation of all the concerned stakeholders in the work of the Working Party, such as private business associations, civil liberties associations, trade unions, consumer protection organisations, academics and all those affected and interested by data protection issues. It is astonishing and regrettable that, just as the national data protection supervisors, the Art. 29 W.P. as the pivot of the debate has not done more important efforts to get their participation in the reflection and assessment processes. Although recently, the Art. 29 W.P. and the Commission have initiated public consultations on specific issues involving stakeholders, including academics and individuals, there is still much progress to be made at this level. Secondly, the Art. 29 W.P. appears to be driven by a still more proactive *attitude* and a pragmatic *strategy* of alliances with crucial actors : it tries to influence the lawmaking process by intervening in the debate as early as possible. Linked to the former, thirdly, the Article 29 W.P. is taking seriously the raising of new *concerns* and issues, related to new developments in the practices of processing of personal data.

B. – *The Hypothesis of 'Reflexive Governance'*

The concept of 'reflexive governance' is closely linked with questions of good governance in the European Union, more particularly

in the field of human rights (102). It tries to answer the question of a common – coherent and efficient – human rights policy in the Union, despite the limits inherent to its constitutional structure. Hypothetically there are two opposite (and extreme) ways to deal with such question. On the one hand such policy and regulatory system could be devised in a top-down and authoritative manner, binding for all, by an entrusted supranational body deemed to represent the common interest and respecting the pre-existing rules and procedures. In that case a policy would be imposed by the supranational authorities through a supranational ruling, leading to uniformisation or harmonisation of the national legal system. On the other hand, such policy could be conceived as the product of a decentralised process and left to a sort of regulatory competition among the local actors, which would have the advantages of the elaboration of policies closely articulated to the local citizens and conditions and the respect of the national sovereignty. However such inter-jurisdictional competition might turn out to be destructive and cannot be assumed to be conducted in the common public interest (especially in a field as human rights) (103). There is no reason to presume that either the first scenario, that of top-down regulation, or the second scenario, of data protection law being the result of a decentralized process of implementation and interpretation of framework rules, will lead to optimal results.

Today in the EU, the implementation and enforcement of human rights happens mainly at the level of the Member States, which is a situation that generates a lot of problems when the objective is

(102) In the next paragraphs we refer to the concept of 'reflexive governance' as it has been determined, explained and elaborated in the Integrated Project *Reflexive Governance in the Public Interest* or REFGOV (6th Community Framework Programme in Research and Development). This research project focuses 'on emerging institutional mechanisms which seek to answer the question of market failures by means other than command-and-control regulation imposed in the name of the public interest. It seeks to identify these new mechanisms of 'reflexive governance', to evaluate them and to make institutional proposals for an improved form of governance'; homepage of the project at http://refgov.cpdr.ucl.ac.be/. We have based our short descriptions on the Working Papers of the project, that are available via http://refgov.cpdr.ucl.ac.be/?go=publications. For a more elaborate description of the hypothesis of 'reflexive governance', see also the introductory contribution by Olivier De Schutter to this volume.

(103) The putting of this dichotomy between regulatory competition and harmonisation/uniformisation is, of course an oversimplification because many interdependencies between the jurisdictions and quite some intermediate forms of coordination (e.g. the 'open method of coordination') do exist. See O. De Schutter, *A fundamental Rights policy in the Public Interest : the Decentralised Implementation of Fundamental Rights in a Single Area*, Working Paper Series : REFGOV-FR1, 2006, 5-8 (available via http://refgov.cpdr.ucl.ac.be/?go=publications).

to work out a fundamental rights policy in the common European public interest. On the other hand, a more centralised uniformisation or harmonisation would imply a new transferral of state powers to the Union. Hence, it is a challenge (the challenge of the REFGOV project) to explore and examine which coordination mechanism could be thought and proposed in order to reach the objective of a fundamental rights policy in the public interest without further transferral of powers from the Member States (104). The hypothesis of 'reflexive governance' intervenes precisely at this point as it posits itself beyond the dilemma between top-down regulation (with transferral of powers) and inter-jurisdictional competition. It seeks to identify modes of coordinative or collaborative governance that focus on processes that permit a 'constructivist' articulation all the concerns at hand, rather than the need to reach a pre-established and pre-defined goal in one way or another. More particularly, the hypothesis of 'reflexive governance', applied in the field of fundamental rights, requires :

> 'the organisation of a *permanent learning process between the actors involved* in the protection and promotion of fundamental rights. Such collective learning should serve two complementary goals in improving the governance of fundamental rights in the Union : it should serve to identify the issues on which collective action is required at the level of the Union; and it should encourage a systematic exchange of experiences in order to contribute to a better informed and more reflexive definition of the policies of pursuing fundamental rights.' (105)

What is crucial in the hypothesis is its focus on the idea that a fundamental rights policy in the public interest can best be build up and devised in a permanent – and thus never achieved – process of collective and mutual learning by all the actors involved, by all the stakeholders. Learning, from this perspective, happens by 'doing', rather than by 'absorbing'. It can no longer be seen as the transmission of 'a pre-existing thing' called knowledge by someone who is assumed to know, to someone who is assumed to be an ignorant. Learning on the contrary then becomes a constructivist and pragmatic process (or perhaps an experiment). Such an approach can of course never be general, passive or static. On the contrary it must focus on the way 'issues' are constructed by all the actors concerned (and not only by one or two institutional players). Such an

(104) *Ibid.*, 2.
(105) *Ibid.*, 2 (our italics).

approach, in other words, requires *for each particular issue*, that a political state of affairs be made by all the stakeholders. Conversely, an issue cannot exist outside the concerns and interest of those affected by it (106). This process would be beneficial for two reasons : it would involve the concerned and affected stakeholders, increasing its legitimacy in democratic terms; and it would inject the knowledge and experience of these stakeholders in the decision-making process and purportedly lead to more informed and effective decisions (107).

C. – *The Art. 29 Working Party : An Illustration of 'Reflexive Governance'?*

The European legal framework of data protection aims at harmonisation or approximation of the national data protection laws in the Member States. The Data Protection Directive sets the principles and purposes the Member States have to attain and implement in their respective legal systems. The purpose of this approach is that the different domestic regulations would be similar enough to take away legal obstacles or barriers for a free flow of personal data

(106) See B. LATOUR, 'Why Has Critique Run Out of Steam ? From Matters of Fact to Matters of Concern', (Winter 2004) 30 *Critical Inquiry* 2, 225-248; and B. LATOUR, 'From Realpolitik to Dingpolitik. How to Make Things Public ?', in B. LATOUR and P. WEIBEL (eds), *Making things public. Atmospheres of democracy*, Chussetts (ZKM-Zentrum für Kunst und Medientechnologie, Karlsruhe/The MIT Press, 2005), 14-41. See also : N. MARRES, *No Issue, No Public. Democratic Deficits after the Displacement of Politics* (2005), p. 175 (Ph.D. Amsterdam), (available via http://dare.uva.nl).

(107) There is an interesting comparison to be made between the hypothesis of 'reflexive governance' and the issue of 'Public proofs – Science, Technology and Democracy' to which the *Society for Social Studies of Sciences* (4S) and the *European Association for the Study of Science and Technology* (EASST) have devoted their common conference of August 2004 in Paris (*Public proofs. Science, technology and democracy*, 4S & EASST conference, Paris, August 25-28, 2004, Centre de sociologie de l'innovation/Ecole des mines de Paris). The organisers of the conference motivated their choice as follows : 'The divide between, on the one hand, experts who could be trusted for their access to indisputable matters of fact and, on the other, the general public waiting for enlightenment and defining societal values, has been erased. (...) Thus, the question of providing public proofs has taken on a new prominence : those proofs inherit all the problems of the former scientific proof, but, in addition, they have to take into account all the problems of providing agreement'.

(http://www.csi.ensmp.fr/WebCSI/4S/index.php). Hence, 'public evidence' must meet two conditions. On the one hand it must be based on robust knowledge (knowledge that resists controversies and tests within the relevant scientific community); on the other hand it must assemble, gather and convince the concerned citizens and publics, and allow for agreement and assent. The organisation of public evidence, thus, should involve a double set of constraints : those of robust scientific knowledge and those set by the concerned publics. As regards the latter, these should include all those that will suffer or enjoy the consequences of the introduction of new scientific artefacts. See also, in the same vein, M. CALLON, P. LASCOUMES and Y. BARTHE, *Agir dans un monde incertain. Essai sur la démocratie technique* (Paris, Seuil, 2001), 358.

in the single area. In other words : the objective to enforce a 'high level' of data protection in all the Member States (108) is closely intertwined with the objective to realise the 'free movement' of personal data in the Union (109).

Of course, this approach bears a non hypothetical but very tangible risk of discrepancies amongst the domestic data protection legislations. Such discrepancies can find their origin in many factors related to differences in economic and privacy policies, in constitutional and legal systems (110), in pre-existing data protection laws, in more concrete technical transposition of principles, etc. As has been said already, the main task of the Art. 29 W.P. is precisely to reduce the risk of discrepancies among the national implementations of the Data Protection Directive; it has the task 'to contribute to the uniform application of the national measures taken to implement the data protection directive' (art. 30 Data Protection Directive). Hence it acts as an advisory body, a messenger and a mediator in the interspaces between the European and domestic levels of governance, and between the different national policy makers, legislators and data protection supervisors. We view this institutional position of the Art. 29 W.P. and the way it carries out its task as very relevant from the perspective of thinking of the concept of 'reflexive governance' in relation to the decentralised implementation of a fundamental right. This is obvious because the Art. 29 W.P. has been specifically established to meet two ends, namely the protection as such of the fundamental right to data protection and its decentralised but coordinated implementation in the European Union.

On one hand, indeed, the Art. 29 W.P. and the National Data Protection Authorities have been established with a view to better protect the rights included in the Data Protection Directive and in the 'fundamental right to data protection' as enshrined in Article 8 of the EU Charter of Fundamental Rights. It is

(108) See the tenth preliminary recital of the Data Protection Directive.

(109) See S. GUTWIRTH, *Privacy and the information age*, cited above, 91-95.

(110) Not all countries have, such as Belgium, linked data protection to privacy. Countries such as France and Germany, lacking an explicit right to privacy in their constitution, have searched and found other legal anchors for the recognition of data protection rights. French data protection is therefore based on the right to liberty, whereas German data protection is based on the right to have human dignity recognized. See P. DE HERT and S. GUTWIRTH, 'Privacy, data protection and law enforcement', cited above, 81-82.

hence the very *raison d'être* of such institutions to compensate for the given *imbalance* of power between the data controllers and the data subjects. Their first appeal is to be a watchdog of the respect of the data protection rights of the data subjects (because, to put it bluntly, the data controllers know very well how to protect their own interests). On one hand, thus, the Data Protection Authorities and the Art. 29 W.P. must gain *public trust*, and contribute to an effective implementation of the fundamental right to data protection respectively at national and European level.

On the other hand the Working Party has been explicitly conceived as a body contributing to the 'coordination' and 'uniform application' of the national measures implementing the Data Protection Directive in the Member States. From this perspective it participates in coordinating and devising the different national data protection policies in the light of the Data Protection Directive, not being a 'top-down' authority issuing binding opinions or rules but by listening to the different voices in the light of the principles enshrined in the Data Protection Directive, by being a meeting and coordinating place for representatives of the different national D.P.A.'s, by constructing consensus opinions, by anticipating new problems, and so on, as we discussed above.

All this shows, we believe, that the Art. 29 W.P. can be definitely seen as a good illustration of a way – there are certainly others – of giving institutional form and substance to the hypothesis of 'reflexive governance' in the field of human rights. Our analysis of the work, working methods, strategies and achievements of the Working Party do effectively show a continuous, pragmatic and constructivist learning process by all the protagonists involved. It is by learning from the others, both externally and internally, by taking into account inputs from key players (such as European Commission and Parliament, the European Court of Human Rights, etc.), that questions are framed and answered in such way that they fit in the very complex cobweb that makes data protection exist as a dynamic fundamental right. This is no minor task since the Art. 29 W.P. has a double role to play as a 'watchdog' denunciating privacy threats and having a non neutral position in favour of privacy and data protection

interests, and simultaneously, as an independent authority in charge of administrative tasks and searching for compromises and consensus. Such a double role can only be successfully played through a cautious step by step and case by case approach, in which listening to concerns and carefully articulating them is quintessential.

It can however be deplored that the Art. 29 W.P. has not widened the extent of its actions to the wider circle of stakeholders, including civil society movements and business representatives. If the process of 'reflexive governance' refers to a never ending process of collective learning which *ideally* involves *all* the actors concerned of affected by the issue at stake, namely data protection, it must become a priority for the Art. 29 W.P. to seriously involve the stakeholders in its deliberative processes. The launching of online consultations is certainly a step in this direction, although this way of proceeding might be considered as lacking a dimension in active dialogical participation.

We believe that our expectations are neither exaggerated nor unrealistic. On the contrary, they match with the way issues already emerge and are politically and legally dealt with. Take for example the highly debated and contested issue of the transfer of European PNR-data (*Passenger Name Records*) to the United States Department of Homeland Security for purposes linked to the 'war on terrorism'. Without going into any detail, who were the protagonists of this issue? Who were the actors involved and concerned? Who did participate to the construction of the issue? As a matter of fact the list is very long. Let us just mention some of the players involved, without going into any more details : 1. the US-Government, the European Commission and Council of Ministers, the Governments of the Member States; 2. the European airline companies that were put under high pressure by the United States Government; 3. some national Data Protection Authorities and the Art. 29 W.P. who issued critical opinions about the adequacy of the protection of personal data in the US; 4. the EDPS who eventually imposed his voice in the debate; 5. the European Parliament and especially its *Committee on Citizens' Freedoms and Rights* who not only opposed but also filed two successful actions with the European Court of Justice against the decisions taken by the Com-

mission and the Council (111), and who has consulted e.g. representatives of civil society organisations and academics concerned by the issue; 6. A number of concerned and committed civil society organisations voicing their opposition like EPIC, Privacy International, Statewatch, the International Federation for Human Rights that often took up the important role of bell-ringers; 7. academic writers who shined their critical light on the issue and were heard in many assemblies; 8. the Court of Justice, first through the opinion of Advocate General Léger, and later, through its judgment; 9. the victims of 'mismatches' of the *Computer Assisted Pre-screening Program* ('CAPPS II'), who were stigmatised as suspects and/or denied access to their flights; 10. the EU Network of independent experts on fundamental rights ...

The former shows that an issue such as the transfer of PNR-data is extremely complex and ramified. It implies that the widening of the involvement of stakeholders in the decision-making processes pertaining to data protection, and especially in respect of the work of the Art. 29 W.P., is certainly not only a requirement following from a theory or hypothesis, it is also very realistic and pragmatic. In practice, the collective learning process is ongoing because actors are *de facto* interested and concerned by the issue they are building, the point of good governance being to really involve the participation of those many concerned and interested actors into the relevant policy discussions and decisions. We believe that the example of the Art. 29 W.P. can teach us a lot on that point, although there is still and still will be a lot of learning that lies ahead.

(111) Notably, actions respectively against the Council of Ministers and the Commission, seeking the annulment of respectively the agreement between the European Community and the United States; and the Commission Decision on the adequate protection of the PNR data transferred to the U.S., see the joined Cases C-317/04 and C-318/04 of 30 May 2006, note 30, via www.curia.eu.int.

ANNEX : Art. 29 and 30 Data Protection Directive

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall :

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall 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.