Transborder data flows and extraterritoriality

Poullet, Yves

Published in:
Journal of international commercial law and technology

Publication date:
2007

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

Transborder Data Flows and Extraterritoriality: The European Position[1]

Yves POULLET
Prof. at the Faculties of Law of Namur and Liège
Director of the CRID
Yves.poullet@fundp.ac.be

Abstract. This paper will discuss the issue of whether the EU Privacy regulatory framework, in respect of the first pillar, has an impact beyond the EU frontiers, as well as the fundamental principles regarding extraterritoriality of EU Laws.

Introduction

The questions I have to deal with might be summarized as follows. Does the EU Privacy regulatory framework in respect of the first pillar [2] have an impact beyond the EU frontiers? If so, what are the fundamental principles regarding extraterritoriality of EU laws?

In order to answer these questions, I will start with a brief reminder of the historical background of the present EU Privacy regulation on transborder data flows (TBDF): From article 8 of the European Convention (ECHR) to the TBDF issues. Thereafter, we will analyse more deeply the extraterritorial impacts of the two main EU Directives: the first one, dated from 1995[3] , and called the General Directive and the second one, dated from 2002[4], which is a more specific directive on "Electronic Communications and Privacy".

[1] This paper reflects the personal views of the author and does not necessarily reflect the positions of any affiliated institution.

[2] The distinction between the three pillars of the European Union is quite important insofar as different procedural rules must be followed for the adoption of EU regulations according to these pillars. The present EU Privacy Directive is only applicable to the first pillar (Community) and not to the second pillar (External relationships) or the third pillar (Interior Security, Police and Judicial cooperation). Regarding the Second pillar, in Article 11 of the TEU, it is stated: "1. The Union shall define and implement a common foreign and security policy covering all areas of foreign and security policy, the objectives of which shall be: -to safeguard the common values, fundamental interests, independence and integrity of the Union in conformity with the principles of the United Nations Charter,-to strengthen the security of the Union in all ways,-to preserve peace and strengthen international security, in accordance with the principles of the United Nations Charter, as well as the principles of the Helsinki Final Act and the objectives of the Paris Charter, including those on external borders,-to promote international cooperation,-to develop and consolidate democracy and the rule of law, and respect for human rights and fundamental freedoms". As far as the Third pillar is concerned, Article 29 states: "Without prejudice to the powers of the European Community, the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters and by preventing and combating racism and xenophobia.. That objective shall be achieved by preventing and combating crime, organised or otherwise, in particular terrorism,(…)". The European Union envisages to enact 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). This Decision will introduce in the Third Pillar the same concepts as in the first and will definitively extend the same regulatory framework regarding TBDF as provided by the 1992 Directive on Data Protection On that point, see the European Data Protection Supervisor (EDPS) opinion available on the EDPS website : http://www.edps.europa.eu/ .

[3] 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 and on the free movement of such data O. J,L 281 , 23 Nov.,1995 P. 0031 – 0050.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J No L 201, 31 July 2002. Article 3§1 states: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community".

I. From European Convention on Human Rights (ECHR) to the TBDF issues[5]

It is helpful to begin with a few considerations about the Council of Europe and the EU approaches to privacy protections.

Council of Europe Approach

For the Council of Europe, article 8 ECHR[6] explicitly enumerates privacy as a fundamental human right. This right was conceived in 1950 mainly as the protection of intimacy, in other words, a "right to opacity"[7] intended to ensure the protection of sensitive data. Progressively, the right to privacy has become the right to self-determination. It means the possibility for everyone to determine for him/herself the way to find his or her way in the society. This extension has been made possible because the Convention is deemed a "living instrument", which ought to be interpreted only in an extensive way (see on these points, notably Tyrer[8] and Selmouni[9]cases).

Further progressive development here leads one to consider that the protection of all data, what might be viewed as "the informational image of the individuals", has to be ensured, and not only the sensitive data. On that point, the Rotaru Case [10]decided on May 4, 2000 by the European Court of Human Rights might be referred. According this decision, article 8 ECHR might cover all personal data including those of public nature when these data are processed systematically and automatically.

Having defined very broadly the scope of the "privacy" right, the Court adds that its protection must be "practical and effective" and must not be kept as "theoretical and illusory" (Airey, 1979) .[11] As discussed in the following sections, this assertion is very important in the context of the TBDF regulation.

Finally, the Council of Europe does consider that the State is the first guarantor of its citizens' data protection. The State is the ultimate guarantor of human rights and freedoms: « the State has a positive obligation to ensure that everyone within its jurisdiction enjoys in full, and without being able to waive them, the rights and freedom guaranteed by the Convention. » (Refah, 2003) [12]

This role envisioned for the State means that the States do not only have a negative obligation not to interfere with Privacy (except definitively in the strict conditions of article 8.2.), but also have an an overall positive obligation to ensure that their citizens' privacy will be protected vis-à-vis third parties - this protection is thus available against private bodies (companies or associations) or persons located in third countries insofar our Privacy might be put at risk by the processing operated by these data controllers[13]. This is the main reason why

---

[5] See already our findings in Y.POULLET, "le droit et le devoir de l'Union Européenne et des Etats membres de veiller au respect de la protection des données dans le commerce mondial.", in The Spanish Constitution in the European Constitutional Context, F.SEGADO (ed.), Dickinson S.L., Madrid, 2003, p. 1753 and ff.5 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no.:108, Strasbourg 28-01-1981. Available at: http://conventions.coe.int/treaty/en/Treaties/Html/108.htm

[6] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no.:108, Strasbourg 28-01-1981. Available at: http://conventions.coe.int/treaty/en/Treaties/Html/108.htm

[7] According to the expression of P.DE HERT and S.GUTWIRTH, "Privacy, Data Protection and Law enforcement, opacity of the individuals and transparency of power, Privacy and Criminal Law, (E.CLAES, A.DUFF and S.GUTWIRTH(ed.), Intersentia, Antwerpen-Oxford, 2006, p. 61 and ff.

[8] ECtHR, 25 April 1978, Tyrer v. UK, § 31; See also, ECtHR, 22 Oct. 1981, Dudgeon v. UK, § 60 and more recently, ECtHR, 4 Feb. 2005, Mamatkumlov a.o. v. Turkey. EHCR, 28 July 1999.

[9] EHCR, 28 July 1999, Selmouni v. France, § 100 On that case Law, read, R.A. LAWSON, "the monitoring of Fundamental Rights in the Union as a Contribution to the European Legal space : the role of the European Court of Justice, in Proceedings of the first REFGOV Open Conference, O. de SCHUTTER (ed.), May 2006, Brussels, to be published.

[10] EHCR, 4 May 1999, Rotaru v. Romania. Application no. 28341/95. On this decision and the article.8 enlargement to all personal data, see O.de SCHUTTER, Vie privée et protection de l'individu vis à vis des traitements de données à caractère personnel, Rev. Trim. Dr.h., 2001, p. 148 and ff..,

[11] ECtHR, 9 Oct. 1979, Airey v. Ireland. See also ECtHR, 23 March 1995, Loizidou v. Turkey.

[12] ECtHR, 31 July 2001, Refah Partisi v.Turkey.

[13] We have to bear in mind that otherwise, member States would be passive of liability for violation of the European Convention on Human Rights (ECHR). [define]. See supra: D. YERNAULT "L'efficacité de la Convention Européenne des Droits de l'homme pour contester le système 'Echelon'", in Sénat et Chambre des Représentants de Belgique, Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé 'Echelon' , Feb. 25, 2002. Yernault studies the nature of the ECHR: (1) as an instrument guaranteeing "European public order", considered as a coherent whole, in the sense that it was qualified by the Strasbourg Court in 1995; (2) as an international treaty that gives place to the State's international liability; and (3) as an

Convention n° 108 and all European Legislation have been adopted creating a public regulatory framework enforceable not only in the public sector, but also in the private sector, including regulating explicitly the TBDF[14].

European Union Approach.

As regards the EU approach, it is important to note that the European Union has only been declared competent as regards human rights protection and regulation since the Treaty of Amsterdam in 1997. This Treaty refers extensively to the European Convention of Human Rights by asserting [15] that the EU has to guarantee the respect of the human rights enumerated by the ECHR.

The European Court of Justice in the Loizidou case[16] has explicitly recognized the European Convention as a "constitutional instrument of the EU public order", having the priority on all other international (e.g. the WTO Agreements) and national legislation of European or other foreign countries according to ECJ decision in the Matthews case17

To take fully in consideration the extension of the scope of Article 8 ECHR with regards to privacy, the EU Charter on Human Rights adopted in 2000 by the Treaty of Nice[18] has distinguished the Data Protection from the Privacy Right in order to consecrate the right of each EU citizen to have all his or her personal data protected: firstly, by limiting the processing of these data only to legitimate purpose, including their consent; secondly, by granting to the data subject a right to access; and thirdly, by recognizing to the Data Protection Authorities a prominent role for ensuring the respect of the different data protection (DP) principles[19].

Having recalled the development of privacy and data protection rights, we might now envisage the specific attitude of our EU authorities vis-à-vis the TBDF. However, before further analysis on that topic, it is important to identify and distinguish two situations where European personal data are at risk due to the TBDF, which are discussed in the next section.

---

international treaty of a particular nature, due to its Article 53, by virtue of which adherent States recognise its legal pre-eminence over any other internal or international regulation that would be less protective of Fundamental Rights than the Convention itself.

[14] It seems that this intervention of the States in protecting Privacy distinguishes fundamentally the US and EU approach. On that point, see C.MANNY: "When European state that Privacy is a fundamental right, the effect among American is to frame questions of consumer information Privacy in terms of Privacy interests of individuals against organisational or societal interference." ("European and American Privacy Commerce, Rights and Justice", in Proceedings of the Academy of Legal studies, Business Conference, Albuquerque, New Mexico, Aug. 2001 and J. REIDENBERG, "The background and underlying philosophy of the European Directive differs from that of the United States. While there is a consensus among democratic society that Information Privacy is a critical element of civil, society, the US has, in recent years, left the protection of privacy to markets *rather than law. In contrast, Europe treats privacy as a political* imperative anchored in fundamental human rights." (J. REIDENBERG, "E-Commerce and Trans-Atlantic Privacy", 38 Houston Law Review,2001, p. 731.)

[15] A recent trend from ECJ to make a systematic reference to the Jurisprudence established by the European Court of Human Rights is quite noteworthy in that respect (see e.g. the E.C.J. K.B, case (C-1171/01) Jan. 7, 2004 and the Pupino case (C-105/03), June 16, 2005).

[16] Already quoted footnote 10

17 ECtHR, 18 Feb. 1999, Matthews v. UK

[18] Full text of the Charter of fundamental Rights of the European Union, OJEC C 364/1, 18-12-2000 available at : http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf. 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://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp26en.htm. This article has been taken again in the Draft EU Constitution (art. 50)submitted to the President of the European Council in Rome on 18th July 2003, available at: http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf . Even if, for the time being, the Charter is not legally binding, its philosophy affects the three Pillars of EU law. The Charter stresses the nature of privacy and data protection as fundamental rights within the European Union and individualise each one, pointing out their autonomy. That proves that they are essential concepts for the EU policy design, and constitute part of European public order.

[19] Article 8: Protection of personal data: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.3. Compliance with these rules shall be subject to control by an independent authority."

II. A fundamental distinction between two kinds of TBDF: Is the Directive 95/46 regime insufficient?

The first TBDF situation is traditional and obvious. A person, company, or administration located in Europe is exporting data for various reasons, e.g. to perform a contract on behalf of his/her customer, to ensure in a third country the processing of certain technical applications (back up or storage of data), or to build up a common data base concerning employees located in different countries.

The second situation is less obvious: due to the global nature of the modern networks and the absence of infrastructure frontiers, the processing operated by persons located outside of the EU might directly affect our privacy by sending spyware, transmitting data to third parties through invisible hyperlinks or addressing unsolicited mails through the web.

These last examples are quite different from the first ones, as the privacy risks are caused by parties located in third countries without the data necessarily having been transferred consciously by data controller located within Europe.

The distinction between the two TBDF hypotheses will lead to different provisions. The first situation is regulated by the General Directive and its two main principles asserted by the Recital, n° 56 and 57:

> " Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;
> Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited. " »

In other words, the Directive recognizes the importance of positive TBDF input in the development of the commerce. At the same time, it underlines the EU commitment to ensure the protection of the Privacy considered as a Human Right and thus justifies the legitimate restrictions and conditions embodied in Articles 25 and 26, as quoted above.

A related question has recently been raised before the European Court of Justice, the famous *Linqvist* case [20], in the context of a web site created by a European citizen and revealing and containing data about third parties. Insofar as the web site might be consulted from terminals located outside of Europe, can we consider that the EU Data Directive provision on TBDF are applicable? The European judges answer by the negative, but this negative answer is founded on weak arguments. Even if the website is not as such exporting data by his/her conscious operation and although he/she has deliberately created the risk of exportations by placing personal data on his/her website. articles 25 and 26 are arguably applicable.

Alternatively, certain other situations might not very easily fall under the application of the articles 25 and 26 of the so-called General Directive insofar they are not the consequences of a directly or indirectly voluntary data transmission by a person located in Europe. In this respect, I just will quote the "*Echelon* case" [21], insofar it is a question of the third pillar. In this case, due to the characteristics of the communications by satellite, both the US and the UK governments have developed a system of electronic surveillance which are able to read satellite communications including those sent by a person located within Europe to another European citizen. It was thus possible for the UK and US Intelligence Services to spy on European citizens, companies or administrations, whose communications were circulating through satellites, without trespassing the E.U borders. The European Parliament [22], six days before the 11th of September nightmare, strongly reacted to these new privacy threats and violation of its sovereignty by claiming the adoption by the E.U of new tools in order to better ensure its citizens'

[20] ECJ Nov. 6 2003,published notably in RDTI,2002,4 ,p. 145 and ff. C. de TERWANGNE, : Affaire Linqvist ou quand la Cour de Justice des Communautés Européennes prend position en matière de protection des données personnelles See also M.V. PEREZ-ASINARI and Y. POULLET, "Privacy, Personal Data and the Safe Harbour Decision", in The future of Transatlantic Economic Relations,(ANDREWS, POLLACK, SCHAEFFER (ed)), Robert Schuman Centre for advanced Studies, 2005, p. 101 and ff.

[21] This case has been revealed by different documents like J. BAMFORD's one: "The puzzle Palace" or N.HAGER's one "The Secret power". The STOA (Advisory Committee of the EU Parliament on Technology Assessment) has published different reports on ECHELON

[22] EU Parliament Resolution, Sept. 5, 2001.

privacy and its sovereignty [23]. Six days later , that claim was forgotten due to the overwhelming sympathy for the Americans.

In this case, the transmission outside of Europe is the result of the global and interactive nature of the networks used by the European residents. However, there was no transfer in the sense of the 1995 Directive.

The present development and growth of the Internet infrastructure also potentially ensures a global and interactive circulation of all messages. This situation leads the E.U to enact, in 2002, a specific Directive as regards "Data Protection and the electronic communications sector" in order to face these new risks. In this respect, we will analyse the provisions of the Directive 2002/58, which implicitly but definitively regulate certain activities of data controllers notwithstanding the fact they are located inside or outside of Europe. So, activities like electronic communications interceptions, use of traffic or location data, and sending unsolicited communications are under the EU regulations even if they are operated from outside the European Union.

The following reflections will thus analyse separately the two situations.

III. TBDF and the Directive 95/46

The basic principles of the TBDF regime

The basic principle regarding the territorial scope of the Directive 95/46 is reflected in article 4.1, which provides in part that the Directive is applicable if and only if "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State". The criterion to determine the geographical scope of the Directive is thus the physical link between the data processor's activities and the EU territory, where the real activities of the data processor are taking place.[24] On this point, we might conclude that data transmission to third countries are regulated, even if the TBDF provisions have an impact outside European borders. To have an extraterritorial impact does not mean that legislation has an extraterritorial scope of application. Concerning the question of extraterritoriality in the age of Globalization, it has been recently been specifically pointed out by a Canadian Report[25] that "in some cases, measures are designed to have extraterritorial reach by influencing the actions of other Nations." For example, the European Data Protection Directive specifically provides that EU member states must legislate so that there could be no trans-border movement of data for processing abroad, unless the target country had enacted legislation establishing substantially equivalent data protection norms. Although such legislation would have no overt extraterritorial reach, the threat of loss of trade as a result of the Data Protection Directive was a strong motivating factor for the Canadian Government's decision to enact the Personal Information Protection and Electronic Documents Act."

Only one exception [26] is foreseen by the Directive: "The Directive is applicable when the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State… " In this case, the Data controller located outside of the European Community has an obligation to designate a representative established in the territory of that Member State. Several commentators [27]have underlined the ambiguous meaning of this provision.

---

[23] These points are broadly developed by the SCHMID report on the existence of a global system for the interception of private and commercial communications (Echelon interception system), report presented at the Temporary Committee on the Echelon interception system settled up by the European Parliament, May 18, 2004. About the ECHELON surveillance system, see D.YERNAULT, "De la fiction à la réalité: le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'Homme", Rev. b. dr. Intern., 2000, p. 134 and ff..

[24] …Establishment does not mean necessarily where the data processing occurs About the meaning of this criterion and the explanation of this choice by the European Directive, see .L.A.BYGRAEVE, « Determining applicable law pursuant to European Data Protection Legislation », in E-Commerce Law and practice in Europe, C.WALDEN and J.HÖRNLE (eds), Woodhead Publishing Limited, Cambridge, 2001, p. 4 and ff. and from the same author, Data Protection: Approaching its Rationale,Logic and Limits, Doctoral thesis, Oslo, 1999 published by Kluwer Law international, 2000.

[25] S.COUGHLAN, R.J. CURRIE, H.M. KINDRED, T. SCASA, Global reach, Local Grasp: Constructing extraterritorial jurisdiction in the Age of Globalization, Report addressed to the Law Commission of Canada, June 23, 2006.

[26] Reguarding Article 4.1(c), see the assertion stated by TERSTEGGE : "This rule leads to some odd extraterritorial side effects." ("Directive95/46/EC, art. 4" in Concise European IT Law, (A.BULLESBACH, Y.POULLET and C.PRIENS (eds.)), Kluwer Law Int., 2006, p. 164).

[27] The Article 29 Working Party discussing about the meaning of this provision recommends a cautious application of this article, which should be applied only in cases "where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved.(Article 29

Either, the provision is just making a reference to the articles 25 and ff., or this article deals with cases of remote automated processing apart from controllers outside of EU (cookies, spyware, etc.) and intends to invoke the application of the Directive to processing done under the total control of Data controllers located outside of Europe. In other words, the criterion to be applied is the master ship of the functioning of the equipment.

The better view[28] would require that this second interpretation must be followed. The provision refers precisely to cases where a data processor located outside of Europe has or takes the full control of the equipment located in Europe and so makes use of this equipment, collecting by this use directly within this equipment certain data without voluntary authorization or without conscious transmission by the terminal equipment possessor. Cookies or spyware are examples of these collections of data directly generated by remote usage of equipment, but we might also think about pre-programming certain applications, which permits direct access from outside to certain data files without authorization of the data possessors. It is quite clear that in these circumstances, the extraterritorial applicability of the Directive might be considered as a way to prevent the specific risks linked with this kind of transmission insofar the articles 25 and ff. are not applicable. As discussed below, article 4.1.c) might be considered as a pre-figuration of the new provisions enacted under the Directive 2002/58.

The TBDF regime

Let us come back to the main TBDF principles, which are applicable only to data controllers located within the EU territory. The TBDF is forbidden unless "adequate protection" is offered by the recipient of the flow located in a third country. According to the famous "Methodology Paper", adopted by the Article 29 Working Group in '98 [29], the concept of "adequate protection" has to be distinguished from other concepts like the concepts of "equivalent protection" or "sufficient protection". Indeed, according to the "Methodology Paper", "adequate protection" does not mean neither "equivalent protection", neither sufficient protection which means a lower level of protection unacceptable by European Union .

Equivalency would have required a strict analytical comparison between two documents of similar nature, *i.e.*, between the foreign legislative Act and the EU one. In other words, the criterion of an equivalent protection would have apparently required the adoption by the third country of legislation, which might be considered—more or less - as a copy of the Directive.

With the "adequate protection" requirement, the question to be solved is different and might be expressed as follows: considering the specific privacy risks linked with a TBDF and taking into consideration the number and quality of the data transferred, the types of usages pursued by the transfer, the eventual onward transfers, etc., can we consider that the protection of the data subjects is or not effectively ensured following the main requirements of the EU directive.?

The approach takes into account the conformity of the object of the protection, meaning the content of the protection afforded by the regulatory environment of the TBDF, and its effectiveness. If it is important that the regulatory provisions surrounding the TBDF- no matter their nature (self-regulatory, contractual or legislative nature)- assert the security, access, fairness and proportionality principles, it is even important that the data subjects might take benefit of support and assistance mechanisms in order to ensure that these principles are respected, and that their complaints might be suited, investigated, judged and enforced by really independent, easily accessible and competent authorities

Thus, the EU approach is very open [30]

Firstly, it forbids any judgment a priori. The fact that a country has ratified the Convention n° 108 is not per se a guarantee that the country offers an adequate protection. A case by case approach is needed taking into account fully the characteristics of the flow to be analyzed and the protection effectively offered by the recipient. The use

[28] See, M.H. BOULANGER and C.de TERWANGNE, "Internet et le respect de la vie privée", in Internet face au droit, Cahiers du Centre de recherches Informatique et Droit, n° 12, 1997, p.211 .L.A.BYGRAEVE, « Determining applicable law pursuant to European Data Protection Legislation », in E-Commerce Law and practice in Europe, C.WALDEN and J.HÖRNLE (eds), Woodhead Publishing Limited, Cambridge, 2001, p. 4 and ff.

[29] 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, WP 12, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

[30] About this approach, Y. POULLET, B. HAVELANGE, A. LEFEBVRE, "Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel" Rapport final, Centre de recherches Informatique et Droit, Univ. Of Namur, Belgium, EU Commission, DG XV, December 1997.

of the term "adequate" is meaningful and perfectly translates the pragmatism of the European approach that might be characterized as not ideological or theoretical.

Secondly, this attitude is the contrary of any EU imperialism[31] regarding the way by which the protection would have to be ensured. Under articles 25.2 and 26.2 wording, any regulatory way 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 pinpoint the EU Commission Decision in 2000 about the adequacy of the US "Safe Harbour Principles"[32].

Thirdly, the European approach has to be viewed as a "functional" and "risk oriented" approach. The question to be addressed in case of a TBDF might be expressed a follows: "Which kind of mechanisms effectively might protect against the precise risks linked with the TBDF at stake?"

The "effectiveness" and "conformity" of the protection might be ensured by various regulatory methods implies the existence of a complaint's mechanism and the possible intervention if needed of an independent authority (though not necessarily a public one, it might be a private ADR). This authority must have competence to investigate and to pronounce dissuasive sanctions. All these conditions of effectiveness might eventually be realised in the context of a self-regulatory system like a code of conduct. This focus on effectiveness explains that recently, the Article 29 Working Group has judged that the adequacy offered by the US "Safe Harbour Principles" might be questioned not because of the self-regulatory nature of the protection afforded but because its lack of actual effectiveness [33]. According to this approach, the EU competent authorities have multiplied the ways whereby an adequate protection might be offered.

The first way under article 25 al. 2 is definitively the regulatory (at the broadest sense) environment surrounding the activities of the recipient and available in the recipient's country, whatever the regulatory quality of this environment. On that respect, let us add that in order to prevent discrepancies between the attitudes of the different Member States, the EU Commission might intervene, according to the articles 25.4 and 6 (the "white" or "black" lists' systems), by a decision in order to substitute to national decisions, a European one34.

Article 26.1 joins together different exceptional cases [35]where due to the very specific nature or the precise content of the TBDF, no major privacy risks do exist.

Contractual provisions between the sender and the recipient might offer appropriate security measures under art. 26.2 [36]. According the article 26.4., contractual models have been proposed by the EU Commission [37].

---

[31] Y. POULLET, " Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données" in Ceci n'est pas un juriste- Liber Amicorum B. de Schutter, M. Cools and alii (eds), VUB Press , 2003, p. 242 and ff.

[32] Commission Decision 2000/520/EC, July 26, 2000, 0.J. Aug.25, 2000, L.275,p. 7 and ff.

[33] 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. BYGRAEVE, Safe Harbour Decision Implementation Study, at the request of the E.U Commission, published on the web site of the Commission: http://ec.europa.eu/justice_home/fsj/privacy

34 A complete list of the decision taken by the Commission under this provision is available at the EU Commission website: http://ec.europa.eu/justice_home/fsj/privacy/ .

[35] A set of derogations to the general principle is enacted by the Directive, so the transfer will be possible when:

"(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.".

It must be noted that all these derogations must be interpreted restrictively.(On that interpretation, see Article 29 W.P., "Working Document on a common interpretation of art 26(1) of Directive 95/46/EC of 24 October 1995" , adopted on 25 November 2005, WP 114.

[36] « A Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses ».

Finally, considering the organisational specificities of the multinational companies, it might be possible to take benefit of these specificities (internal audit, common privacy policies, and corporate sanctions) for guaranteeing an adequate protection, as proposed by the Article 29 Working Group in 2005 [38]. The solution will consist in enacting Binding Corporate Rules (BCR),that means a common Privacy Policy available in all the establishments of the multinational company and which must be enforceable through legal but also and overall organisational mechanisms.

Apart from the considerations, we might address certain findings about the TBDF regime set up the Directive 95/46. Definitively through these different documents, one might pinpoint the main concerns expressed by the E.U. Most of the attention is put on the "effectiveness" of the protection afforded, no matter the regulatory instrument chosen. This effectiveness is obtained both by the responsibility given to the European data transmitter[39].who will have to take in charge the consequences of the privacy violation and ultimately by the possibility of judicial recourse by the data subjects before an EU jurisdiction applying the EU Data Protection Directive's provisions.

TBDF regime and WTO

The great suppleness [40] used to appreciate the "adequate protection" is definitively a good thing, but it might also lead to risks of discrimination between third countries. For example, Australia might consider that it is discriminatory if the EU Commission refused to consider its legislation as not adequate while, at the same time, accepted the "US Safe Harbour Principles."

This risk of a discriminatory application is coupled with a great risk concerning a lack of effective control by the national authority as regards the quality of the instruments offered for the recipient. How does one control whether the privacy policy taken by a multinational company as IBM is really applied by the different IBM national subsidiaries? The resources of the DP Authorities in controlling all TBDF are definitively insufficient[41].

Another criticism is addressed by the private sector to the DPA. The absence of a unique locket and the diversity of attitudes between each of them create problems for companies operating in different when they have to introduce demands for TBDF.

In conclusion, one might speak about a real extraterritorial impact of the directive. No provisions contained in this directive, except the case foreseen in art. 4.1.c, might be analyzed as having an extraterritorial scope. The

---

[37] 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 - O.J. L 181/19 of 4.7.2001. Available at: http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf; Commission Decision (2002/16/EC) of 27 December 2001on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC. Available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_en.pdf; and more recently the Commission Decision C (2004)5271 of 27 December 2004 0.J. L 385/74 of 29.4.2004amending the Decision 2001/497/EC of 15 June 2001 on alternative clauses.

[38] Document de travail: Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, 03.06.2003, WP 74

[39] See the obligation under art. 25 of the transmitter to check the existence of the adequate protection offered by the third country; the provision about the joint liability of the sender in case of violation by the receiver in the contractual clauses and in the C.B.R., the responsibility supported by the EU subsidiary participating within a multinational company having adopted these C.B.R..

[40] "The interest in privacy contracts is timely given the growing complexity and dynamic nature of the global information economy and information society. This interest should not be dismissed as mere politics, or as a means of gracefully acknowledging the different philosophical approaches to achieving privacy protection between jurisdictions. The issue of personal privacy requires a multilateral approach using a variety of mechanisms tailored to the particular environments in which they must operate." E. LONGWORTH, "Contractual Privacy Solutions." 22nd International Conference on Privacy and Data Protection, Venice, 27-30 September, 2000. "Contracts are, as such, a way for contracting parties to self-regulate their relationships. It might also be a way for one of the party to enforce vis à vis the other one a self-regulatory solution."; Y. POULLET, "How to regulate the Internet: New Paradigms for the Internet Governance." In E-Commerce law and practise in Europe. Edited by I. WALDEN and J. HORNLE under the auspices of the ECLIP Network. Woodhead Publishing Limited. Cambridge, England, 2001

[41] As pointed out by the Article 29 Working Group in its "Declaration of the Article 29 Working Party on Enforcement", adopted on 25th November 2004, W.P.101

targeted situations are only ones clearly located in Europe, as regards the actors targeted and the operations they are undertaking.

TBDF regime and web sites: A challenged ECJ decision

Regarding the Directive 95/46 and its provision about TBDP, a second point must be studied, particularly in the context of a recent decision taken by the European Court of Justice in 2003: the famous Linqvist case.[42]

A Swedish parochianhas created a web site containing useful information especially for the parochians, but including personal data (Members of the Parochy's council, contact addresses, etc) including sensitive ones (notably the disease of one member of the Parochy's council). Among the prejudicial question raised by the Swedish Court to the E.C.J. was the following one: "Are the articles 25 and 26 of the D.P. Directive applicable to web sources"? The European Court's answer is negative, but its arguments might easily receive objections[43] .

Under the judges' opinions, TBDF means active transmission towards third countries and not consultation apart from abroad. This distinction between "transmission" and "consultation" remains from a technological point of view quite ambiguous. What is the difference between, on one side, the situation where a sender, through his/her computer programming, send data to a recipient or, on the other side, the one where by another programming, the sender makes accessible certain data to this recipient. The difference between the "push" and the "pull" systems[44] makes no sense, except if the sender has no technical possibility to avoid the transfer by blocking the access. It should be noted that in this exceptional case, the directive would be applicable under article 4.1.c, as previously explained. In the case of a web site, accessible through the Internet, the creator of this web site has willingly made the data fully available and has the possibility to restrict the access.

The second argument is still weaker. Following the judges in Linqvist, if a data transfer exists, it occurs from the hosting service and not by the web site creator. This argument might not be accepted. The hosting server is not a data controller but a data processor insofar he is acting on behalf of the web site creator. Anyway, this argument does not contradict the existence of a TBDF,

The last point is undoubtedly the major argument. In the context of the worldwide web development, each possible consultation of a web site would be considered as a TBDF and so the TBDF rules would become a general rule, impracticable insofar the web site's visits might happen from all the countries and would require an analysis of all national regimes. If this analysis is negative as regards certain countries, an effective and selective implementation of its outcomes would be required.

On that point, however, it might be opposed that the TBDF rules contain already a long list of exceptions available in most of the websites, [45]where creation does constitute a result of his/her author's freedom of expression. The European Union's approach provides the need to balance in an appropriate way the Right to Privacy and this Right to a free expression without regard to border frontiers. [Of course, there are still problems of differential rules on expression, as the Yahoo! Case in the United States has explored.].

Having taken into account these exceptions which considerably reduce the weight of the ECJ's arguments, it must be recognized in favour of an application of the TBDF provisions that the publication on web sites of certain information and their availability throughout the world create definitively a major privacy risk which justifies the application of the articles 25 and 26. So, we might imagine that certain duties of care[46] would be imposed to the website creators and to their hosting providers and that the possibility of intervention [47]by the public authorities ought to exist in case of major risks, for example if it is proved that people from a third country are systematically analysing the profiles of individuals apart from their presence on the web in order to take actions against them or to publish their profiles.

---

[42] ECJ Nov.6 2003, published notably in RDTI, 2004, 2, 145, note C. de TERWANGNE: Affaire Linqvist ou quand la Cour de Justice des Communautés Européennes prend position en matière de protection des données personnelles

[43] M.V. PEREZ-ASINARI and Y. POULLET, "Privacy, Personal Data and the Safe Harbour Decision", in The future of Transatlantic Economic Relations,(ANDREWS, POLLACK, SCHAEFFER (ed)), Robert Schuman Centre for advanced Studies, 2005, p. 101 and ff.

[44] The Article 29 Data Protection Working Party has expressed the same view in the famous PNR case. See Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States, 24th October 2002, WP 66, p. 7. Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 13th June 2003, WP 78, p. 7. For a clarification on "applicable law" issues see: Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 30 May 2002, WP 56.

[45] On that point, see our reflections in M.V. PEREZ ASINARI and Y. POULLET, op. cit., p. 101.

[46] So, by avoiding the posting of sensitive data, by imposing certain restrictions of access, …

[47] …by blocking the access to websites to certain visitors nominated or coming from certain countries.

IV. The Directive 2002/58 and the TBDF

As previously discussed, this directive fully takes into consideration the recent development of Internet services and the global nature of its infrastructure. As regards the nature of the privacy risks linked with TBDF, the International and global infrastructure of the Internet presents risk for its European users far beyond the specific risks generated by the operations of Trans-border Data Flows by data controllers established in E.U. countries. Moreover due to the fact that Internet, and more generally all telecommunications networks, are offered on a worldwide basis, the European Union has to take into account the global character of these networks. As it has been revealed by the recent Echelon case [48], privacy threats against data covered and protected by the European Union directives might occur in the cyberspace by data controllers located outside Europe. It would be ineffective to restrict the European Union Protection to the European Borders. For example, more than 60 percent of the web sites are located in U.S. It is thus crucial to envisage the protection of European Internet users surfing on web sites located in U.S.

The traffic or location data might be transmitted and processed unlawfully by Telecommunications services providers established outside of the E.U. European Data subjects might be victims of unsolicited mails or by illicit and unfair data collected through cookies or spyware installed on their hard disks by processors established anywhere throughout the world. Therefore, the provisions of the Directive 2002/58 target all Electronic communications services without taking into account the nationality or the establishment of their providers. In that sense, one might speak clearly about the extraterritoriality of this Directive[49].

The obligation for any provider to respect the opt-in system as regards unsolicited communications, even if his/her own national legislation, foresees the opt-out system, like the US Spam Act. Article 5.3., which severely limits the use of electronic communications services for providing access to information stored into the terminal equipment, is applicable to all electronic communications services providers no matter where these providers are established. Other examples might be given.

The global nature of networks restricts the effective scope of the provisions of this Directive. This position does represent a clear answer to the disappearance of the national borders. "But in the 21st Century, border security can no longer be just a coastline, or a line on the ground between two nations. It's also a line of information in a computer, telling us who is in the country, for how long, and for what reason? In the 21th Century it is not enough place to place inspectors at our ports of entry to monitor the flow of goods and people. We must also have a 'virtual border' that operates far beyond the land border of the United States"[50].

V. The European TBDF regime and the WTO rules

Our reflections lead naturally to the following questions. Is the twofold European TBDF regime compatible with WTO rules? Especially, is the extraterritorial application of Directive 2002/58 in compliance with WTO rules? The question might be raised for other national Privacy legislations like the 1998 US COPPA (Children Online Privacy Protection Act) or the 2003 US SPAM Act, which also have extraterritorial effects. It has been explicitly raised before and solved by the WTO appellate body in a decision concerning the US legislation on Internet Gambling [51]. The same arguments might be applied here.

---

[48] About Echelon, the global surveillance system of satellite communications and the European Debate thereabout, see J-M. DINANT- Y. POULLET, Le réseau Echelon, Existe-t'il ? Que peut-il faire ? Peut-on et doit-on s'en protéger?, Rapport rédigé pour à l'attention du Comité permanent de contrôle des services de renseignements, March 7, 2000, published in the annual report of the « Comité permanent de contrôle des services de renseignements », 2000, p. 13 and ff.

[49] "Some of the services covered by the Directive might be offered to a subscriber or a use inside the European Union from a provider located outside the Community, for example as Internet access provider, In that case, the text states clearly that the European Directive is applicable. The criterion fixed by the Directive is not the same as the criterion of establishment retained by the General Directive and will thus permit an extraterritorial effect of this Directive." (Y.POULLET, "Directive 2002/58/EC, art. 4", in Concise European IT Law, (A.BULLESBACH, Y.POULLET and C.PRIENS (eds.)), Kluwer Law Int., 2006, p. 164.

[50] This declaration has been pronounced in the PNR context. This reasoning has been also held in the context of the ECHELON case quoted above.

[51] On that decision, M.V. PEREZ-ASINARI," Internet gambling and betting services: When the GATS' rules are not applied due to the public morals/public order exception. What lessons can be learnt?", CL&SR, 2006

The Dispute Settlement Body of the W.T.O. in a first moment and the Appellate Body in a second time [52] were requested to solve the dispute between Antigua and US concerning the limitations created by various U.S. laws, including the Wire Act, upon cross-border provision of Internet Gambling and betting services. The "public morals" exception was invoked by US. The WTO Appellate Body's opinion might be summarized as follows. Effectively, the Wire Act and the measures taken under this basis affect directly the cross border supply of gambling services through Internet. These measures, to be acceptable, must be necessary to protect public morals or to maintain the public order, under Act XIV of the GATS. In other words, "the public order exception might be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of the Society".

The WTO Appellate Body considers as "vital and important at the highest degree" the necessity of the Wire Act. That necessity is due to the peculiarities of the remote supply of gambling services by the Internet which put at additional risks the US Internet user. Finally, the WTO Appellate Body underlines the absence of reasonable alternative existing for the US legislator in order to ensure the defence of national values.

Apart from the reasoning held by the WTO judges in this gambling case, one might conclude that despite its extraterritorial impact or dimension and its effects on the free cross border market, the provisions on TBDF enacted by the Directive 95/46, which definitively have an extraterritorial impact, and the extraterritorial scope of application of the Directive 2002/58 would be considered as not infringing the WTO rules.

Indeed, Privacy is expressly mentioned in art. XIV of the GATS as a possible exception to this free cross-border market if no arbitrary or unjustifiable discrimination exists. The WTO Preamble also highlights the importance "of giving due respect to national policy objectives" and "the right of (WTO) Member States to regulate and to introduce new regulations, on the supply of services within their territory in order to meet national policy objectives …)". At this respect, nobody will contest that Privacy is considered by European Union and most of the Constitutions of EU Member States as a Human Right and its protection is deemed a matter of "public order." Moreover, as previously said under the ECHR case law, it is the absolute duty of the European Union Members States to ensure this right effectively in the new ICT context and to give the absolute priority to the EHCR rules vis-à-vis any other rules, including international commitments and conventions, like WTO[53].

Nevertheless, it remains necessary to check if the European Union does respect the limits imposed by the WTO to the implementation of this public order exception. Recently, PEREZ ASINARI[54]has proposed a "four-steps-methodology" in applying the exceptions of privacy and public order. That methodology is under her opinion perfectly respected by the EU in the context of the Directive 95/46. Particularly, she pinpoints the fact that the EU has justified fully the restriction imposed by the article 25 and 26 in underlining how it would be easy to circumvent the EU Data Protection laws by transferring the data to third countries offering no or less protection. The measures might so be deemed as "necessary to secure compliance" with the EU public national objectives. Furthermore, the EU has developed precise criteria by the famous Working Paper n° 12 of the Working Group [55] to assess the adequacy of the solutions proposed by the recipient and the sender in order to offer an adequate protection. The respect of these criteria and the motivation of each decision as regards the quality of the protection offered by a third country ensures that the measures will not be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction of international trade"[56]. Perhaps , we might add that the contractual and Binding Corporate

---

[52] WTO, Appellate Body Report, United States - Measures affecting the Cross-border Supply of Gambling and Betting Services, WT/DS285/AB/R, April 7, 2005, available at: www.wto.org/english/tratop.e/dispu_e/285abr_e.pdf.

[53] J.H.H. WEILER, " Fundamental rights and territorial boundaries: On Standards and Values in the protection of Human Rights", in The European Union and Human Rights, N.A. NEUWAHL and J.J. ROSAS (eds), Dordrecht, Martinus Nijhoff Publishers, 1995, p. 51 and ff..

[54] 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", 9 Electronic Communications Law Review, 2002, 249-280.

[55] 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, WP 12, available at: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

[56] One might not exclude that even if the risks of arbitrary or unjustifiable discrimination are to a great extent reduced by a strict application of this assessment's methodology, there is still a part of subjectivity in this analysis, which might lead in casu to possible discriminatory decision even if the Commission recalls its concern to avoid any discrimination. See, in the US Safe Harbor Decision, the Recital 4 of the Commission Decision says : « Given the different approaches to data protection in third countries, the adequacy assessment should be carried out and any decision based on Article 25(6) of Directive 95/46/EC should be enforced in a way that does not arbitrarily or

Rules (B.C.R). solutions proposed as possible alternatives when no adequate protection is offered by the regulatory regime existing in the third country, enlarge the possible ways for senders and recipients to find an appropriate solution corresponding to their needs.

The extraterritorial scope of the 2002/58 Directive is justified by the necessity of taking into consideration the characteristics of the global and interactive Internet network. Insofar these characteristics multiply the possibility of privacy threats by trans-border and uncontrollable data flows, the EU position and its adoption of certain restrictive measures might be deemed as necessary even if these measures are affecting the cross-border supply of the Internet services. No possible discrimination will exist insofar the EU authorities might intervene towards any infringing service supplier wherever he is located. It might be underlined that no prior authorization for the supply of electronic communication services is required, what would have created major concerns about the proportionality of this regulatory system and would have been judged as discriminatory by giving privileges to the EU suppliers. The obligation imposed to every supplier and the a posteriori intervention even if they have impact on the cross-border trade ought to be considered as necessary to secure compliance with the EU requirements and create no risks of discriminatory application between countries. On this point, we have to mention that this recourse might be quite illusory since the extraterritorial enforcement of the judgment is far from being obvious. .

Conclusions

Recently the Geneva and Tunis World Summits on Information Society (WSIS) has pleaded for "global" norms for privacy: "We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users. ". Even if this global solution is not easy to build up due to the fact that Privacy is definitively enshrined in the cultural, historical and cultural background of each society[57], it seems that no other alternative exists in response to the characteristics of data flows at the digital age.

One might not deny that the European Union is committed and has the obligation under the EU treaties to ensure its residents' privacy as an element of its fundamental Human Right value. This defence might not be ensured as it was the case before the expansion of the Internet, which means in the context of the adoption of the Directive 95/46, by controlling certain TBDF mostly identifiable. Experienced in the very disparate contexts of our daily life, the progressive invasion in our life and in our terminals by the worldwide and ubiquitous Internet technology requires European authorities to adopt new regulatory measures which will be applied notwithstanding the location of the intruder. "Globally and locally, today's information societies are underpinned by digital technologies…Ubiquitous networks are at the heart of the digital age."[58] The adoption of these new measures and their application must fully take into account the legitimate limitations imposed by the rules of the international trade in the same manner this international trade might not alleviate the rules dictated by the public order objectives pursued by the EU authorities in protecting Privacy.

This EU intervention is not per se incompatible with the adoption of an international instrument, which will represent a global consensus on Data Protection. This consensus has been achieved twice in the 80's both at the OECD level and at the Council of Europe level. Recently, as regards another topic, a consensus about the fight against the Cyber criminality[59] has been obtained by the adoption in 2001 of the Council of Europe Convention on Cyber crime signed not only by Europe , but also notably by US and Japan. A precedent might be invoked in the Privacy context insofar as Privacy invasion might to a certain extent be considered as a Cyber crime, which needs to be addressed through international cooperation between different national law enforcement authorities.

---

unjustifiably discriminate against or between third countries where like conditions prevail nor constitute a disguised barrier to trade taking into account the Community's present international commitments. »

[57] As regards this assertion, amongst others, the reflection of J.DHONT and M.V. Perez ASINARI, " New Physics and the Law. A comparative Approach to the EU and US Privacy and Data Protection Regulation .looking for Adequate protection" in L'utilisation de la méthode comparative en droit européen, ,PUN (Univ. of Namur), 2004.. See also, J.Q. WHITMAN, "The two western Cultures of Privacy. Dignity v. Liberty.", 113 Yale Law Journal,(2004), p. 1151 and ff.. In the context of the assessment devoted to the analysis of the Indian, Japanese or other far located countries, we had the opportunity to verify the truth of this assertion.

[58] R. MANSELL, « Human Rights and Equity in Cyberspace », in Human Rights in the Digital Age, KLANG and MURRAY (ed.), Glasshouse Press, London, 2005, p.3.

[59] Council of Europe Convention on Cybercrime Nov. 15th 2001, . It might be added that the violation of the privacy legislation through the Internet might be deemed as a Cybercrime and that the intrusion in a terminal might be qualified to a certain extent as a "hacking" in the sense of the Council of Europe Convention on Cybercrime.

Other authors have proposed the adoption in the context of the WTO the adoption of a "General Agreement on Information Privacy" (GAIP)[60], taking fully into consideration the economic value of the personal data and the impact of their regulation on the International trade. Undoubtedly the economic dimension of the Human right might not be denied. But to what extent would certain countries like to enlarge the WTO competences in that direction? The solution resides in a multilateral and multi-stakeholders' discussion clearly encouraged by the WSIS. It is quite clear that a global approach to privacy would be preferable. UN intervention seems to be required [61] at this stage insofar all cultural, philosophical, social and not only economic aspects must be envisaged in discussing about the Privacy as Human right. Furthermore, it might be recalled that UN has adopted in 1990 "Guidelines on computerized personal data files"[62], according to the Article 12 of the Universal Declaration of Human Rights [63] and might be interested to take new initiatives.

We need this global approach. Trust in our technologies without borders is at this prize.

[60] J. REIDENBERG, « E-commerce and Trans-Atlantic Privacy » , 38 Houston Law Review, (2001), p. 77 and ff. See also, with certain doubts, P. SWIRE and R.LITAN, None of your business. World Data Flows. Electronic Commerce and the European Privacy Directive, Brookings Institution Press, Washington DC., 1998, p. 194.

[61] In that sense also, EU PETERSMANN, " Time for integrating Human Rights into the Law of Worldwide Organizations", Jean Monnet Working Paper 7/01 available at : http://www.jeanmonnetprogram.org/papers/01/012301,rtf.

[62] Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly, Resolution 45/95 of 14 December 1990.

[63] …that stipulates : « No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."