The new transatlantic agenda and the future of transatlantic economic governance : privacy, personal data protection and the Safe Harbour decision. From euphoria to policy

Pérez Asinari, María Veroníca; Poullet, Yves

Publication date:
2004

Document Version
Early version, also known as pre-print

The New Transatlantic Agenda and the Future of Transatlantic Economic Governance: Privacy, Personal Data Protection and the Safe Harbour Decision.

From Euphoria to Policy. From Policy to Regulation...?

by

María Verónica Pérez Asinari* and Yves Poullet**
Centre de Recherches Informatique et Droit (CRID)
University of Namur
Belgium
http://www.crid.be

This paper has been prepared in the context of the Workshop "The New Transatlantic Agenda and the Future of Transatlantic Economic Governance", a Joint Workshop of the European University Institute, The University of Wisconsin, and Johns Hopkins University. Robert Schuman Centre for Advanced Studies, European University Institute, Florence, Italy, 18-19 June 2004.

*Researcher at the CRID. She can be contacted at: veronica.perez@fundp.ac.be
**Dean of the Faculty of Law. Director of the CRID. Professor at the Universities of Namur and Liege. He can be contacted at: yves.poullet@fundp.ac.be

We would like to thank Christophe Lazaro, researcher at the CRID, for his comments on an early draft of this paper.

1. Introduction

International trade took digital form in a sort of technological and market euphoria. Even if the "extreme" euphoria of the 90's has calmed down after the dot.coms crisis this new form of exchange has come to stay with us and became to be the most natural thing.

The advantages of information technologies in regards to multilateral economic relations were early pointed out as a key element of the transatlantic political dialogue. The Transatlantic Agenda mentions the will to create a New Transatlantic Marketplace and a Transatlantic Information Society, both of these in the frame of the third shared goal: "contributing to the expansion of world trade and closer economic relations"[1].

In the context of the digital marketplace, many national and multinational companies export and import personal data on a regular basis, for their management activities (human resources, customer care, direct marketing, etc.). Personal information may even be their raw material for market research, profiling, etc., what can constitute the service itself or an added value to their "product" or "commodity". Apart from this, and due to the architecture of Internet protocols, consumers leave traces while using the net, sometimes consciously (e.g. when they purchase goods or contract services in e-commerce platforms and their name, address and other information is required for the deliverance), sometimes unconsciously (e.g. through the use made by companies of clickstream data, when cookies are placed on their hard drives, when invisible hyperlinks are used, etc.[2]). Thus, personal data, as information on the net, crosses states' borders very easily. It can be re-used for many other purposes than the purpose for which it has been initially gathered. Moreover, assisted by very cheap software, the result of this further data processing contributes to an economically viable result.

Given this reality, any dialogue about the digital marketplace policy must involve a concomitant dialogue on privacy and personal data use policy, due to the risks to certain rights of the individual that an uncontrolled use of personal data can create.

This paper will analyse, first, what were the initial political aims of the EU-US dialogue in the realm of the New Transatlantic Agenda (NTA) and related documents. Secondly, a brief

---

[1] Transatlantic Agenda, available at : http://www.eurunion.org/partner/agenda.htm

[2] J-M. DINANT "Law and Technology Convergence in the Data Protection Field? Electronic Threats on Personal Data and Electronic Data Protection on the Internet", Deliverable 2.2.3, ECLIP, Project funded by the EC, IST programme, available at: http://www.eclip.org/documents/deliverable_2_2_3_privacy.pdf , last visited 31/05/04. J-M. DINANT "Les traitements invisibles sur Internet", *Cahiers du CRID n°16,* Bruylant, 1999, pp. 271-294, also available at: http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html, last visited 31/05/04. C. DUCOURTIEUX and S. FOUCART "Les profileurs du Net traquent les internautes à leur insu", *Le Monde*, 10 May 2002, page 20.

description will be given of the EU and US regulatory choices in the privacy arena, aiming to provide the legal background for framing any effort of joint governance. Thirdly, we will analyse if there have been efforts of joint governance, and if so, how have these efforts worked in practise: the Safe Harbour Decision, whether there have been impediments for a successful cooperation, and if so, what institutions and/or practises have been most effective at overcoming such obstacles. Fourthly, we will assess what concrete steps might the US and the EU undertake in the coming months and years, to strengthen cooperation and attain their common goals. Finally, we will conclude by assessing to what extent policy was translated into regulation (State regulation, co-regulation, self-regulation, regulation through technology).

2. Initial political aims. The NTA's perspective on privacy and personal data protection

The NTA does not specifically mention, in its third shared goal, any reference to privacy or personal data protection. Even when it refers to issues where trade intersects with other concerns, the document points out only the "environment, internationally recognised labour standards and competition policy". Could one imagine that there was no important intersection between trade and privacy or that this concern was still not obvious at the time when the NTA was drafted? We will see that it was not the case.

However, two other political documents highlight an intrinsic relationship between trade and the protection of privacy and personal data: (1) the Joint EU-US Action Plan[3] that accompanies the NTA, and (2) the Joint Statement on Electronic Commerce[4].

The Joint EU-US Action Plan sets out specific actions to which the EU and the US have committed themselves, describing concrete steps to carry out in order to achieve each of the four-shared goals. While addressing the New Transatlantic Marketplace, the document foresees that:

- "[w]e will expand and develop the bilateral Information Society Dialogue, in order to further common understanding of global issues implying access to information services through public institutions, regulatory reforms, and technological cooperation, including the continuation of expert-level discussions in the following areas: (...) commercial communications; privacy and data protection; (...)"[5];
- furthermore, it refers explicitly to "data protection" in the following terms: "[w]e will discuss data protection issues with a view to facilitating information flows, while addressing the risks to privacy"[6].

---

[3] Joint EU-US Action Plan, available at: http://www.eurunion.org/partner/actplan.htm

[4] Joint Statement released in conjunction with the EU-US Summit in Washington, DC, December 5, 1997, available at: http://www.eurunion.org/partner/summit/Summit9712/electrst.htm

[5] Point III.2.(i) -devoted to "Information Society, information technology and telecommunications".

[6] Point III.2.(k)

Clearly said, it means that even if privacy concerns must be taken into consideration, they might not affect disproportionably information exchange. Moreover, despite the fact that this document was supposed to "specify" concrete actions, it seems that this field remained in a "discussion" stage. The will/need to regulate or not regulate the privacy field was not mentioned[7].

The Joint Statement on Electronic Commerce establishes certain guidelines for the global expansion of e-commerce. Some statements are made, as far as governance choices are concerned, that goes in -what could be understood as- either "contradictory" or "complementary" ways. The document stipulates, in the relevant part, that:

- such "expansion will be essentially market-led and driven by private initiative"[8];
- "the role of the government is to provide a clear, consistent and predictable legal framework, to promote a pro-competitive environment in which e-commerce can flourish and to ensure adequate protection of public interest objectives such as privacy, intellectual property rights, prevention of fraud, consumer protection, and public safety"[9];
- "industry self-regulation is important. Within the legal framework set by the government, public interest objectives can, as appropriate, be served by international or mutually compatible codes of conduct, model contracts, guidelines, etc., agreed upon between industry and other private sector bodies"[10];
- finally, the parties agree, among other issues, to work towards "ensuring the effective protection of privacy with regard to the processing of personal data on global information networks"[11].

In this case, the political instrument is more explicit, but fuzzy still. Hence, the document pleads in favour of a co-regulatory[12] model founded on a certain partition of responsibilities

---

[7] The degree of cooperation is quite diverse in the different topics addressed. Very concrete commitments are made in other areas. For instance, in Point III.2.(d) "Veterinary and plant health issues", it is stated that "[w]e will conclude an agreement to establish a framework for determining equivalence of veterinary standards and procedures for all live animals products". Point III.2.(h) "Customs cooperation" declares, in the same line that the previously mentioned one, that "[w]e will endeavour to conclude by the end of 1996 a customs cooperation and mutual assistance agreement between the EC and the US. The agreement should cover: (...)".

[8] Point 3(i)

[9] Point 3(ii)

[10] Point 3(iii)

[11] Point 4(iv)

[12] More recently this partition of responsibilities has also been promoted by the World Summit on the Information Society (WSIS) Declaration of Principles when this Declaration asserts: "The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

a) Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;

b) The private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;

among the State and private parties in the regulatory process. Privacy is one of the key issues for the e-commerce political framework, but there is neither a definitive determination about the regulatory choice to address this important issue, nor the compromise for the signature of an agreement, as is the case in other areas of the NTA[13]. It has to be noted that there is a dual reinforcement: on the one hand the role of the government in those areas where there is a public interest, and on the other, the role of private sector self-regulation in serving also those public interest objectives. Not surprisingly enough, the EU-US debate on privacy and data protection will be played in those extremes (as Internet governance in general[14]), to find an eclectic and not definitive[15] solution: the Safe Harbour (SH) framework.

3. Regulatory choices in the EU and in the US

These political documents above mentioned seem not to have been "naive" when leaving a blurred sensation about the regulatory choice. Indeed, this was (and still is) an intricate political and legal matter, where both parties have taken different roads for regulation. Indeed, this makes joint governance more difficult in this realm. A solution was a must, being information (remarkably "personal" information) the petrol of the digital marketplace. But, have there been truly "joint governance" efforts in the practise? We have to understand first the legal framework of both parties separately, in order to see how the joint political basis was intended to be transmitted into practical and legal solutions, to contribute to the achievement of the NTA third shared goal.

Regulatory choices go beyond the very topic of this paper. State legislation, co-regulation, private sector self-regulation, or technological regulation are the result of historical, cultural, economic, etc., choices of a given society. They are not "good" or "bad" in themselves, they

---

c) Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role;

d) Intergovernmental organizations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues;

e) International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies".

The WSIS has been organised by ITU in Geneva (10-12 December 2003). As previously decided, this first meeting will be followed by a second meeting to be held in Tunis in 2005. The WSIS was the result of difficult, numerous and intense discussions at regional and global level. See : World Summit on the Information Society, *Declaration of Principles. Building the Information Society: a global challenge in the new Millennium*, Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003, available at: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc

[13] See footnote 7.

[14] See: J. BERLEUR, E. BROUSSEAU, M. COIPEL, T. DELMAS, T. DEDEURWAERDERE, T. EWBANK de WESPIN, , I. FALQUE-PIERROTIN L. HENNUY, Ch. LAZARO, C. MAESSCHACK, Y. POULLET, R. QUECK *Enjeux à débattre. Gouvernance de la société de l'information. Loi. Autoréglementation. Ethique,* Actes du séminaire, Namur, les 15 et 16 juin 2001, Bruxelles, Bruylant, , 2002. Y. POULLET "How to regulate Internet : New paradigms for Internet Governance self-regulation : value and limits" , *Variations sur le droit de la société de l'information*, Bruxelles, Bruylant, 2002, pp. 79-114. Y. POULLET "De retour d'un sommet mondial de la societé de l'information", *Revue du Droit des Technologies de l'Information*, no. 18, avril 2004, pp. 5-8.

[15] We will see *infra* why, in our opinion, the SH is not a definite solution.

depend on many other contextual premises and the application fashion to the concrete cases[16]. Comparison of these choices and the results in practise are often conducted in this arena, due to the differences they present, mainly, in the regulation of privacy and personal data protection in e-commerce and other Internet and new technologies applications.[17] In what follows, we will have an approximation to the regulatory solutions the parties under analyses have adopted.

3.1. The European framework

The European Convention for the Protection of Human Rights and Fundamental Freedoms[18] regulates the protection of privacy as follows:

> "Article 8: (1) Everyone has the right to respect for his private and family life, his home and his correspondence."[19]

At supranational level, EU Community law has moved from being a pure economic integration process, to a more comprehensive framework. It has incorporated the protection of human rights, as one of its goals since the adoption of the Treaty of Amsterdam[20]. The draft Treaty establishing a Constitution for Europe [21] has even included the Charter of Fundamental Rights of the European Union. Despite the fact that this instrument is not in force yet, it shows an important advance: the provision of an autonomous fundamental right to the protection of personal data[22], as individuated from the right to privacy[23]. Privacy is no more

---

[16] Based on Summers's doctrine, we do propose a triple test of the legal validity of both self-regulatory norms and public regulations: legitimacy- conformity and effectiveness. On these triple criteria, see our reflections: Y. POULLET, "ICT and Regulation; Towards a New Regulatory Approach", to be published in *Internet Governance*, M. Schelleckens (ed.), Kluwer Law Int.

[17] See: G. SHAFFER "Globalization and Social Protection: the Impact of EU and International Rules in the ratcheting up of US Data Privacy Standards", *Yale Journal of International Law*, Winter 2000, vol. 25, pp. 1-88. 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", in *L'utilisation de la méthode comparative en droit européen*, ed. F. van der MENSBRUGGHE, Presses Universitaires de Namur, Namur, 2003, pp. 67-97. C. MANNY "European and American Privacy: Commerce, Rights and Justice", *The Computer Law and Security Report*, Vol. 19, No. 1, pp. 4-10, and Vol. 19, No. 2, pp. 92-100.

[18] Referred to in Article 6 of the TEU and Article 286 of the TCE.

[19] European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, available at: http://www.echr.coe.int/Convention/webConvenENG.pdf

[20] Treaty Establishing the European Community, available at: http://europa.eu.int/eur-lex/en/treaties/dat/EC_consol.pdf

[21] Draft Treaty establishing a Constitution for Europe, Adopted by consensus by the European Convention on 13 June and 10 July 2003, submitted to the President of the European Council in Rome, 18 July 2003, available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/c_169/c_16920030718en00010105.pdf

[22] Article 8: 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

envisaged only as a way to protect sensitive data and the confidentiality of communications but more broadly and more positively, as a way for ensuring the ability of human beings to their self-determination in an Information Society, where information might be considered as a power for data controllers *vis-à-vis* the data subjects[24].

The exchange of personal data across boundaries was early analysed in the [at that time] EEC from the perspective of the internal market: due to the adoption of privacy and data protection laws in different Member States[25] obstacles to the free flow of data could be created due to the disparity of legislation.

The 80's and beginning of 90's are characterised by the effort to find international solutions: the OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data[26], the Council of Europe Convention no. 108 on the protection of individuals with regard to automatic processing of personal data [27], and the UN Guidelines for the Regulation of Computerized Personal Data Files [28]. We can see that the nature of the instruments is different. Whereas the OECD Guidelines and the UN Guidelines are examples of soft law, Convention no. 108 is the first international binding document. All of them have been the source of the upcoming EU rules.

Some months before the signature of the NTA, Directive 95/46/EC[29] was enacted, in order to harmonise divergent Personal Data Protection legislation in what concerns the protection of fundamental rights and freedoms of natural persons (in particular their right to privacy with respect to the processing of personal data), to fulfil the internal market's requirement of free flow of personal data. As a consequence, it establishes some general principles in order to achieve this goal, describing rights for the data subject and obligations for the data controller when processing personal data.

---

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".

[23]Article 7 : "Everyone has the right to respect for his or her private and family life, home and communications".

[24] On this evolution, see D. SOLOVE, "Conceptualizing Privacy", *90 California Law Review* (2002), pp. 1088 and ss.

[25] Land of Hesse (1970); Sweden (1972); Federal Republic of Germany (1977); Denmark (1978); France (1978); Luxemburg (1979).

[26] OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data, 23 September 1980. Available at: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

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

[28] Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990, available at: http://www.unhchr.ch/html/menu3/b/71.htm

[29] 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, OJEC L 281 , 23/11/1995 P. 0031 – 0050. Hereinafter: "the Directive".

Basically, it foresees that the data subject[30] has the rights to information[31], access[32], rectification, erassure and blocking[33].

The data controller[34] has to respect the data quality principles[35], the legitimacy of processing activities[36], she has to notify the national Data Protection Authority the processing activities[37], and she has to implement appropriate technical and organizational measures[38].

Furthermore, to avoid the circumvention of European law, the Directive has created a mechanism, that consists in a general principle for trans-border data flows (TBDF) and a series of exceptions. Indeed, Article 25(1) of the Directive sets out the principle that Member States shall only allow a transfer to take place if the third country in question ensures an "adequate level of protection"[39]. This basic principle, forbidding any TBDF to countries not offering adequate protection might suffer certain exceptions: (a) certain specific derogations (Article 26(1)); (b) adequacy Decisions (Article 25(6)); and (c) protection taken by the sender and the receiver of the TBDF either by contractual means or by their common subjection to legally binding commitments (Article 26(2)).

Before analysing further the different means to ensure an appropriate protection in case of TBDF, let us make a parenthesis here to analyse, very briefly, the concept of "flow" to determine which situations would be regulated under Article 25(1) . The term is not defined in the Directive. A dictionary defines this term as "[t]he action and fact of flowing; movement in a current or stream; an instance or mode of this. Orig. said of liquids, but extended in modern use to all fluids, as air, electricity, etc."[40] We have the idea of movement and also the

---

[30] The "data subject" is the person to whom the data relates. "Personal data" is defined as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity", Article 2(a) of the Directive.

[31] Article 10 and 11 of the Directive.

[32] Article 12(a) of the Directive.

[33] Article 12(b) of the Directive.

[34] The "data controller" is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law", Article 2(d) of the Directive.

[35] Article 6 of the Directive.

[36] Article 7 of the Directive.

[37] Article 18 of the Directive.

[38] Article 17 of the Directive.

[39] This concept of " adequate protection" has been taken again by the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows CETS No.: 181, Strasburg, 8 November 2001.

[40] *A New Dictionary on Historical Principles*, Ed. J. MURRAY, Oxford at the Clarendon Press, 1901, vol. IV.

connection with things that can go from one place to another without recognising frontiers, like the case of the air. A dictionary of informatics defines more precisely the expression "trans-border data flows" as "[c]irculation internationale par télécommunications des données de toutes natures (économiques, techniques, etc.) posant des problèmes multiples: dépendance vis-à-vis des détenteurs de l'information (banques des données), protection des données et de la vie privée, traitement extraterritorial de l'information entraînant un déplacement de la prise de décision"[41]. It is interesting to see that the concept "international circulation of data by telecommunications" is very broad and can represent multiple situations.

In our sphere, this is the case of a company transmitting a database of clients, of potential customers, of employees, of business contacts, etc., to its partner or branch established outside the EU. It is also the case of a customer transferring her personal data via an e-commerce website located in another country in order to receive a good or service[42]. Yet, is it the case of personal data made available on the Internet, which can potentially be accessed by people in third countries? Does this data "flow" from one country to another? Quite surprisingly, the European Court of Justice (ECJ) has understood this as not being a flow [43].

In a recent decision, the ECJ concluded that "[t]here is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country".

The ECJ based this decision on the fact that Chapter IV of the Directive contains no provision concerning use of the Internet. Furthermore, "[i]f Article 25 of Directive 95/46 were interpreted to mean that there is a transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet".

Coming back to the notion of flow and giving consideration to the technical perspective, each time an Internet user consults a website, information packets are transmitted via routers. If, the final destination of this packet is located abroad (that is, the place of establishment of the

---

[41] M. GUINGUAY and A. LAURET, *Dictionnaire d'informatique*, 5e édition, Masson, Paris, 1992.

[42] Even if this case constitutes a "flow" of personal data, it is not covered by the application of the Directive since the data controller, the person responsible for the website who decides the means and purposes of this data processing, is neither established on the territory of one member state –Article 4.1(a)-, nor is making use of equipment located in the EU –Article 4.1(c)-.

[43] Judgment of the Court of 6 November 2003, Criminal proceedings against Bodil Lindqvist, Case C-101/01. Another problem is the case of "flows" generated by cookies or invisible hyperlinks. Should we apply Article 4.1(c) of the Directive, or both Article 4.1(c) plus the rules on TBDF?

user who consult the website, and who can process[44] the data consulted) the information has been exported, so, there has been an international transfer or flow of personal data.

It is rather astonishing, then, that the Court have not considered this technical reality. Indeed, the way to solve legal problems derived from the application of technology is not the denial of the effects that technical reality cause, but the understanding of the need not to leave the cyberspace in anarchy, and the application of the existing law as far as it is legitimate. For instance, the ECJ could have considered that the exceptions to the application of Article 25(1), as described in Article 26(1) (see *infra*) are almost the same that the requisites described in Article 7[45] of the Directive, which constitute the criteria for making a data processing legitimate. In those cases, then, if the processing activity consists in posting personal data on an open network, given the international character of it, and the fact that due to the technical state-of-the-art this posting implies the possibility that an indefinite number of people located abroad have access (and if desired further process) to this data, information to the data subject about this possibility of global access should be required. With this, the data subject would be more aware about the risks that could arise to her data if not adequately protected.

With the reasoning of the ECJ, if a data controller posts personal data on a website legitimised by Article 7(a) of the Directive (unambiguous consent), the given consent of the data subject would even be "informed" and valid if the controller does not mention the fact that this data can be accessed and further processed in countries where there is no or less protection. Could we really consider this consent as "informed"?

Indeed, the main difference between Article 26(1) and Article 7 is its paragraph (f), which stipulates: "Member States shall provide that personal data may be processed only if: (...); (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1".

When a transfer can not be covered by any of the exceptions of Article 26(1), being the processing legitimate in accordance to Article 7(f), the data controller can seek legitimacy for the transfer in any of the other possibilities offered by the Directive (see *infra*). However, in the case of Internet postings, the other possibilities do not offer a global solution, as is the

---

[44] The notion of processing activity given by the Directive is very broad : "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction", Article 2(b) of the Directive.

[45] Article 7: "Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

case of Article 26(1). These other possibilities offer country or country-sectoral solutions (adequacy Decisions) or controller-to-controller/controller-to-processor specific-case solutions (standard contractual clauses). This does not mean that given the flexibility of Article 25(2) of the Directive, other solutions addressing global issues could not be found.

This finding itself and the concept of "flow" -from a theoretical and practical point of view- deserve, clearly, a deeper analysis. However, we could not avoid mentioning it here, due to the direct implication with the subject of this paper.

Coming back to the notion of "adequate" protection, we have to bear in mind that, this concept has to be linked to the degree of risk a transfer presents and to the nature of the data: "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country"[46].

Directive 95/46/EC does not provide for a definition of "adequacy"[47]. The Article 29 Data Protection Working Party has elaborated a working document which states a list of the principles that are considered to be *sine qua non* for personal data protection and that must be present in a third country system to be considered "adequate"[48]. This document is the basis for the analysis of third countries' "adequacy" conducted by the European Commission. It has to be noted that this document is a guideline, that has not the character of formal law. "Adequacy" should be understood in a dynamic way, evolving together with the evolution of EU law[49].

The Directive also foresees a series of exceptions to this general principle:

A. Derogations of Article 26(1)

There are some cases in which a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection can anyway take place. The Directive creates a set of derogations to the general principle, so the transfer will be possible when:

---

[46] Article 25(2) of the Directive.

[47] See: See J. DHONT and M.V. PEREZ ASINARI "New Physics and the Law .", op. cit., pp. 73-79.

[48] Article 29 Personal Data Protection Working Party, *Working Document Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive"*, WP 12, 24 July 1998. The principles enunciated are the following: purpose limitation; data quality and proportionality; transparency; security; rights of access, rectification and opposition; restrictions on onward transfers; additional principles to be applied to specific types of processing: sensitive data, direct marketing, automated individual decisions; procedural and enforcement mechanisms: good level of compliance, support and help to individual data subjects, appropriate redress to the injured party.

[49] For instance, one may think about the influence of Directive 2002/58/EC in the concept of adequacy. Are the solutions of this Directive to the concrete cases regulated a direct application of the general principles of Directive 95/46/EC? Does this new Directive go beyond the general principles imposing new obligations to data controllers? If this were the case, should "adequacy" be analysed on those grounds? In principle, a positive answer to this last question would be the proper approach.

"(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."[50]

B. Adequacy Decisions

If none of the exceptions mentioned above are suitable for the particular typology of transfers to be conducted, there are other possibilities that can be used to make a legitimate transfer. The European Commission can adopt a Decision in order to declare the "adequacy" of a particular system. The European Commission has issued, so far, seven Decisions under Article 25(6). The "Safe Harbour"[51] has been adopted in this context (see *infra*). It determines that a set of privacy principles and frequently asked questions provide adequate level of protection for personal data transferred from the EU to the US. Decisions have been adopted also concerning Switzerland[52] , Hungary[53], Canada[54], Argentina[55], Guernsey[56], and concerning the transfer of PNR airline passengers data to the US[57].

---

[50] Article 26(1) of directive 95/46.

[51] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJEC L 215/7, 25/08/2000.

[52] Commission Decision of 26 July 2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Switzerland, OJEC L 215, 25/08/2000.

[53] Commission Decision of 26 July 2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Hungary, OJEC L 215, 25/08/2000.

[54] Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJEC L 2/13, 4/01/2002.

[55] Commission Decision of 30 June 2003 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided in Argentina, OJEC L 168, 5/07/2003.

[56] Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, OJEC L 308, 25/11/2003.

[57] Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, C(2004) 1914, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/pnr/c-2004-1914/c-2004-1914_en.pdf .. On this issue see M.V. PEREZ ASINARI and Y. POULLET "The airline passenger data disclosure case and the EU-US debate", *Computer Law & Security Report*, Vol. 20 no. 2, 2004, pp. 98-116. See also, by the same authors, "Airline passenger's data: adoption of an adequacy Decision by the European Commission. How will the story end?", to be published in *Computer Law & Security Report*. Note that this arena exceeds the sole application of Directive 95/46/EC (a first pillar instrument). In the context of the NTA, the second shared goal "Responding to global challenges" states what follows: "[w]e are determined to take new steps in our common battle against the scourges of international crime, drug trafficking and terrorism". Indeed, the PNR case must be treated, in principle, in the context of both first and third pillar (Public security questions).

C. Contractual clauses

There is another alternative way for making a safe transfer as stipulated by Article 25(2) and 25(4). Appropriate contractual clauses can be proposed by the data controller to the Member State Data Protection Authority (DPA) for approval, they can be elaborated by this Authority as "standard contractual clauses" or even by the European Commission. This is the case of a Commission Decision on standard contractual clauses for the transfer of personal data to third countries (to controllers) under article 26(4) of Directive 95/46/EC [58] and the Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC[59]. The use of these clauses is voluntary.

The general Directive is complemented by Directive 2002/58/EC[60], which regulates the protection of privacy in the electronic communications sector. This instrument provides specific rules for unsolicited electronic communications, traffic data, cookies, etc.

In the EU framework, self-regulation is foreseen[61] as a "complement", bringing "added value"[62] to state regulation. The Directive foresees that trade associations or other bodies representing other categories of controllers may submit their Codes of Conduct to the Article 29 Data Protection Working Party for an evaluation of compatibility with the Directive.

The Interinstitutional Agreement on better law-making[63] concluded recently by the European Parliament, the Council and the Commission adopts the following approach: "16. The three Institutions recall the Community's obligation to legislate only where it is necessary, (...). They recognize the need to use, in suitable cases or where the Treaty does not specifically require the use of a legal instrument, alternative regulations mechanisms". Notwithstanding, the limit of this approach is determined in the next paragraph: "17. The Commission will ensure that any use of co-regulation or self-regulation is always consistent with Community law and that it meets the criteria of transparency (in particular the publicising of agreements) and representativeness of the general interest. These mechanisms will not be applicable where fundamental rights or important political options are at stake or in situations where the rules must be applied in a uniform fashion in all Member States. They must ensure swift and flexible regulation which does not affect the principles of competition or the unity of the

---

[58] 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, OJEC L 181/19, 4/07/2001.

[59] 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.

[60] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJEC L 201 , 31/07/2002.

[61] Article 27 of the Directive.

[62] The Directive insists about the fact that specificities of each sector must be taken into account in the drafting of Codes of Conduct.

[63] European Parliament, Council and Commission Interinstitutional Agreement on better law-making, OJEC C 321/1, 31/12/2003.

internal market". This approach reaffirms the orientation of the Directive concerning alternative regulatory means[64].

3.2. The US framework

The US regulatory system is noticeably different to the EU one. It is a sort of "patchwork" of federal and state constitutional law, federal and state statutory law, tort law, and industry self-regulation[65]. At international level, the US has signed, but not ratified the American Convention on Human Rights[66] (Pact of San José, Costa Rica), which stipulates the right to privacy in its Article 11[67]. At national level, the US Constitution does not provide explicitly for a right to privacy. However, it foresees different mechanisms to protect the citizens against state intrusion (but not against private entities[68]). The US system of privacy and personal data protection is characterized, then, by fragmentation. There is no general framework covering every sector (private and public, as is the case of the Directive, or Convention no. 108) creating general rights, obligations and the figure of an independent authority (analogue to the European national DPAs). Indeed, the US has not translated internally the trend created by the OECD Guidelines.

Reidenberg and Schwartz underline that "[c]onstitutional rights in the United States forbid government from doing certain things in a certain fashion, but usually do not require the state to take action. The Constitution does not compel the government to create data protection that allocates the burdens and benefits of the state's information use"[69]. The authors identify four critical areas of US Constitutional law of Data Protection[70]: (1) associational privacy; (2) voting rights; (3) the Fourth Amendment's protection against search and seizure; and (4) informational privacy. They analyse these areas *vis-à-vis* four elements of the European approach[71] to data protection searching for functional similarity. It is summarized, then, that:

---

[64] For a broader discussion see: Y. POULLET, "ICT and Regulation ', *op. cit.*

[65] See : P. SCHWARTZ and J. REIDENBERG, *Data Privacy Law. A Study of United States Data Protection,* Michie Law Publishers, Virginia, 1996. J. DHONT and M.V. PEREZ ASINARI "New Physics and the Law...", *op. cit.* Electronic Privacy Information Center and Privacy International, *Privacy & Human Rights*, USA, 2003.

[66] Convención Americana sobre Derechos Humanos, Pacto de San José de Costa Rica, 7 al 22 de noviembre de 1969. Available at : http://www.oas.org/juridico/spanish/tratados/b-32.html . This Convention has been adopted in the context of the Organization of American States (OAS), and it has been ratified by all the Latin American countries, see: http://www.oas.org/juridico/spanish/firmas/b-32.html

[67] Article 11. Right to Privacy: "1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks."

[68] "Most of the private sector's data processing will not be subject to constitutional constraints" P. SCHWARTZ and J. REIDENBERG, *Data Privacy Law. Law..., op. cit.*, p. 31.

[69] P. SCHWARTZ and J. REIDENBERG, *Data Privacy Law. op. cit.*, p. 31

[70] P. SCHWARTZ and J. REIDENBERG, *Data Privacy Law. op. cit.*, p. 36.

"[t]he first two areas of constitutional law, associational privacy and voting rights, are directly related to deliberative democracy. The state's application of personal information regarding group affiliation and exercise of the franchise can harm individual participation in political self-government. Fairly strong constitutional protections exist in these two areas. As for the Fourth Amendment's protection from unreasonable searches and seizures and the Fifth and Fourteenth Amendment's creation of a right of informational privacy, these areas of constitutional law concern deliberative autonomy, or the impact of the state's collection and application of personal information on the individual's ability to make decisions in deciding how to live her life. Here, the Supreme Court's definition and application of these constitutional rights have provided less than satisfactory protection"[72].

Many specific laws have been adopted both for the public and private sector, such as: Fair Credit Reporting Act (1970), Fair Credit Billing Act (1974), Privacy Act (1974), Equal Credit Opportunity Act (1974), Right to Finantial Privacy Act (1978), Computer Matching Act (1988), Video Privacy Act (1988), Electronic Communications and Privacy Act (1986), Cable Communications Policy Act (1984), Telephone Consumer Protection Act(1991), Health Insurance Portability and Accountablity Act –HIPPA-(1996), Children's Online Privacy protection Act –COPPA-(1998), Can Spam Act (2003), etc. It has to be noted that this regulatory model leaves certain sectors unregulated[73].

Further to this, the *Restatement (Second) of Torts*[74] has classified privacy torts as follows: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light privacy; and (4) misappropriation of name or likeness for commercial purposes. It has to be noted that, whereas in the EU data subjects can theoretically introduce a tort law action in case of any personal data protection legislation infringement that results in physical or moral damage, US tort law in the privacy arena is limited to the cases mentioned[75]. Whilst the application of US privacy torts in the digital sphere remain dubious, Annex IV to the Safe Harbour Decision contains an answer to the European Commission's request for clarification of US law with respect to claims for damages for breaches of privacy: "In the context of the safe harbour framework, 'intrusion upon seclusion' could encompass the unauthorized collection of personal information whereas the unauthorized use of personal information for commercial purposes could give rise to a claim of appropriation. Similarly, the disclosure of personal information that is standard of being *highly offensive to a reasonable person.* Finally, the invasion of privacy that results from the publication or disclosure of *sensitive personal information* could give rise to a cause of action for 'publication of private facts'."[76]

---

[71] The four elements have been schematised as follows: "(a) the establishment of obligations and responsibilities for personal information; (b) the maintenance of transparent processing of personal information; (c) the creation of special protection for sensitive data; and, (d) the establishment of enforcement rights and effective oversight of the treatment of personal information". P. SCHWARTZ and J. REIDENBERG, *Data Privacy Law..., op. cit.,* p. 13.

[72] P. SCHWARTZ and J. REIDENBERG, *Data Privacy Law..., op. cit.,* p. 43-44.

[73] See : See J. DHONT and M.V. PEREZ ASINARI "New Physics and the Law .", *op. cit.*, pp. 84-89.

[74] Restatement of the Law Second, Torts 2d, § 652, Division St Paul, Minn., American Law Institute Publishers, 1977, pp. 376-403.

[75] J. DHONT and M.V. PEREZ ASINARI "New Physics and the Law...", *op. cit.*, p. 89

[76] Italics added. We see that, even in the off-line world the application of these torts is quite restrictive.

As far as the particular field of e-commerce is concerned[77], the White House issued a political document, during Clinton administration, giving guidelines for the regulatory approach[78]. The document develops the following statements: (1) the private sector should lead, (2) Governments should avoid undue restrictions on electronic commerce, (3) where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce, (4) governments should recognize the unique qualities of the Internet, and (5) electronic commerce over the Internet should be facilitated on a global basis. In what concerns privacy it applies the same principles, being in line with the general philosophy of the paper: "[t]he Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy."[79]

So far, the federal government has considered the e-market regulatory failure, in what concerns the protection of on-line children's privacy, what derived in the adoption of COPPA. Apart from that, even if, in a certain moment the Federal Trade Commission has pointed out the necessity to adopt legislation to protect consumer privacy on the Internet[80], the FTC chairman referred that more study was necessary before the adoption of legislation in this field[81].

That being the case, self-regulation is the US choice for the protection of privacy and personal data in the e-commerce context. There is a burden in the data subject's side, she has to check what is the level of privacy each of her digital interlocutor offers. Protection is not provided by default. There is no legal obligation to provide protection, unless the US data controller (a website administrator, the company representative, or the person/body with legal capacity to oblige the company) has represented to guarantee it. Then, if there is a misrepresentation, the data subject (the "consumer" in the US conception) can sue for "unfair and deceptive" practice under the FTC Act[82]. The industry has then self-regulated via the adoption of privacy policies posted on their websites, codes of conduct, adhesion to privacy networks (such as NAI[83] or OPA[84]), adoption of labelling systems (such as TRUSTe[85] or BBBonline[86], etc.).

---

[77] See: J. REIDENBERG, "Restoring Americans' Privacy in Electronic Commerce", 14 *Berkeley Tech. L. J.* 1999, pp. 771 and ss.

[78] The White House, *A Framework for Global Electronic Commerce*, July 1997, available at: http://www.nyls.edu/cmc/papers/whgiifra.htm , last visited 31/05/04.

[79] Ibidem.

[80] Privacy Online : Fair Information Practices in the Electronic Marketplace : A Federal Trade Commission Report to Congress (May 2000), available at : http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, last visited 07/06/04

[81] Protecting Consumers' Privacy : 2002 and Beyond, Remarks of FTC Chairman Timothy J. Muris, October 2001, available at: http://www.cdiaonline.org/mediaroomdocs/ACF3194.pdf, last visited 07/06/04

[82] Federal Trade Commission Act, 15 U.S.C. §§ 41-58, as amended. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in the marketplace.

[83] Network Advertising Initiative, see: http://www.networkadvertising.org/ , last visited 31/05/04.

[84] Online Privacy Alliance, see: http://www.privacyalliance.org/ , last visited 31/05/04.

Certain significant problems, which indeed are not circumscribed to the US in their effects, have come to surface in the digital world: "Internet privacy has remained the hottest issue of the past few years. Several profitable companies, including eBay.com, Amazon.com, drkoop.com, and Yahoo.com have either changed users' privacy settings or have changed privacy policy to the detriment of users. A series of companies, including Intel and Microsoft, were discovered to have released products that secretly track the activities of Internet users. Users have filed several lawsuits under the wiretap and computer crime laws. In several cases, TRUSTe, an industry-sponsored self-regulation watchdog group, ruled that the practises did not violate its privacy seal program. Significant controversy arose around online profiling, the practice of advertising companies to track Internet users and compile dossiers on them in order o target banner advertisements. The largest of these advertisers, DoubleClick, ignited widespread public outrage when it began attaching personal information from a marketing firm it purchased to the estimated 100 million previously anonymous profiles it had collected. (...)"[87].

One of the issues that has been creating a major concern is the question of unsolicited commercial e-mails or unsolicited bulk e-mails (generally known as "spam"). The CAN-SPAM Act of 2003[88] has been adopted to tackle this problem. Indeed, this topic can serve as another example to show the different conceptions. Whereas, in Europe, this is an issue that is regulated by privacy laws[89], in the US, this recent Act does not make reference to privacy or personal data protection, but mainly to the monetary costs implications for recipients and Internet Access providers.

Interestingly, this US law has extraterritorial application. For instance, it punishes whoever "accesses to a *protected computer* without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer"[90]; or "uses a *protected computer* to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as the origin of such messages"[91]. A "protected computer" is defined as a computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States"[92]

---

[85] See: http://www.truste.org/ , last visited 31/05/04.

[86] See: http://www.bbbonline.org/ , last visited 31/05/04.

[87] Electronic Privacy Information Center and Privacy International, *Privacy & Human Rights, op. cit.*, p. 530.

[88] Public Law 108–187, 108th Congress, An Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet. 16 December 2003 [S. 877], available at:
http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

[89] Directive 2002/58/EC.

[90] Sec. 4(a)(1), emphasis added.

[91] Sec. 4(a)(1), emphasis added.

[92] Sec. 3(13).

Apart from that, Section 12, "Restrictions on other transmissions", stipulates another extraterritorial application: "Section 227(b)(1) of the Communications Act of 1934 (47 U.S.C. 227(b)(1)) is amended, in the matter preceding subparagraph (A), by inserting `, or any person outside the United States if the recipient is within the United States' after `United States'."

Conscious of the factual limits of a national law in the this domain, the Act acknowledges , in the Section dedicated to the "Congressional findings and policy", that "[t]he problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well"[93].

4. Have there been efforts of joint governance?

When Directive 95/46/EC came into force, certain scholars predicted a sort of catastrophe or trade war in case Article 25(1) of the Directive was enforced[94]. A US civil servant has even declared that such a European regulation would be challenged at the WTO[95].

Clearly, a solution was required. A negotiation process started, then, based on a set of SH Principles and Frequently Asked Questions (FAQs) elaborated by the US Department of Commerce (DoC) jointly with representatives from the private sector. The reasons for the adoption of the SH could be summarized as follows:

- It was clear that the US system could not be considered "adequate" from the EU perspective. Lacunas arise from the different fragments of US regulation. Even in those sectors regulated by statutory law, personal data of EU origin is not always granted the protection described in the Working Document no. 12 (for instance, the Privacy Act is only applicable to "citizen[es] of the United States or an alien lawfully

---

[93] Sec. 2(12).

[94] P. SWIRE and R. LITAN, *None of your Business. World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, Washington D.C., 1998, p. 44.

[95] Ira Magaziner – former responsible person for US discussions on e-commerce-, has declared that she would " challenge EU privacy rules under the theory that they represent barriers to trade", see *"Notes from the OECD Ministerial Meeting on Electronic Commerce"* at Ottawa, Ontario, Canada, October 9, 1998, J. LOVE, Consumer Project on Technology, available at: http://www.cptech.org/ecom/ottawa.html, last visited 31/05/04. Some authors have also referred to that possibility: P. SWIRE and R. LITAN, *None of your Business..., op. cit.*, p. 188-196. L BERGKAMP "The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy", Computer Law & Security Report, vol. 18 no. 1, 2002, pp. 39-40. For another view see: G. SHAFFER "Globalization and Social Protection...", *op. cit.* G. SHAFFER "Managing US-EU Trade Relations through Mutual Recognition and Safe Harbor Agreements: 'New' and 'Global' Approaches to Transtlantic Economic Governance?", EUI Working Papers, RSC No. 2002/28, Robert Schuman Centre, 2002, available at: http://cadmus.iue.it/dspace/retrieve/1606/02_28.pdf .M.V. PEREZ ASINARI "Is there any Room for Privacy and Data Protection within the WTO Rules?", *Electronic Communications Law Review*, vol. 9, 2003, pp. 249-280. 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?", BILETA Conference, *Controlling Information in the Online Environment*, Institute of Computer & Communications law, Queen Mary, University of London, 14-15 April 2003, available at: http://www.bileta.ac.uk/03papers/perez.html

admitted for permanent residence"[96]). The self-regulatory approach, as such, did not give evidence of covering all the "adequacy" principles.

- The Hungarian and Swiss models were not suitable for an adequacy Decision for the US. Those countries do have general data protection systems and they are both signatories of the Convention no. 108.

- Beyond the Directive, Member States have a positive obligation to safeguard the protection of fundamental rights[97].

- However, the flow of personal data is necessary from an economic point of view: there are many economic sectors that conduct trans-border data flows from the EU to the US. Moreover, the EU had assumed political compromises, with the US, by the adoption of the NTA, and also legal compromises at the WTO[98] (and even if privacy is foreseen as an exception to the application of the GATS[99] rules, for this exception to proceed certain requisites must be respected[100]).

---

[96] The Privacy Act of 1974, 5 U.S.C. § 552a (it regulates records handling by Federal, State or local government agencies).

[97] D. YERNAULT "L'efficacité de la Convention Européenne des Droits de l'homme pour contester le système 'Echelon' ", in *Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé 'Echelon'*, Sénat et Chambre des Représentants de Belgique, 25 Fébrier 2002. In this article, the author 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 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. See also: Y. POULLET "Le droit et le devoir de l'Union européenne et des états membres de veiller au respect de la protection des données dans le commerce mondial", *in The Spanish Constitution in the European Constitutional Context*, ed. F. FERNANDEZ SEGADO, Dykinson S.L., Madrid, 2003, pp. 1753-1772.

[98] For studies about WTO implications see : G. SHAFFER "Globalization and Social Protection...", *op. cit.* G. SHAFFER "Managing US-EU Trade Relations through Mutual Recognition and Safe Harbor Agreements...", *op. cit.* .M.V. PEREZ ASINARI "Is there any Room for...', *op. cit.* M.V. PEREZ ASINARI "The WTO and the Protection of Personal Data...", *op. cit*

[99] General Agreement on Trade in Services, available at: http://www.wto.org/english/tratop_e/serv_e/2-obdis_e.htm

[100] Article XIV: "General Exceptions: Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:

(a) necessary to protect public morals or to maintain public order;
(b) necessary to protect human, animal or plant life or health;
(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:

(i)the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;

(ii) *the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;*

After more than two years of negotiations between the US Department of Commerce and the European Commission, the Safe Harbour Decision was issued on the basis of Article 25(6) of the Directive. In the meantime, the industry played an active role expressing its position in this regard, the Article 29 Data Protection Working Party elaborated many Opinions[101] on the level of "adequacy" that the Principles and FAQs represented pointing out certain flaws, and the European Parliament questioned and seriously criticized the (draft) SH Decision[102].

However, as we will see below, the SH was a very punctual effort. It tries to find an exception to the application of Article 25(1) of the Directive, but its application is quite restrictive.

4.1. Characteristics of the Safe Harbour

The "Safe Harbour"[103] (SH) is not an "Agreement" from a Public International law or European Community law perspective[104]. It is a Decision[105], adopted unilaterally by the

---

(iii) safety", emphasis added.

[101] See Article 29 Personal Data Protection Working Party: *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, WP 15, 26 January 1999; *Opinion 2/99 on the adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19 April 1999*, WP 19, 3 May 1999; *Opinion 4/99 on the frequently asked questions to be issued by the US Department of Commerce to the proposed "Safe Harbor Principles"* , WP 21, 7 June 1999; *Working Document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles"*, WP 23, 7 July 1999; *Opinion 7/99 on the level of data protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce*, WP 27, 3 December 1999; *Opinion 3/2000 on the EU/US dialogue concerning the "SH" arrangement*, WP 31, 16 March 2000; *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*, WP 32, 16 May 2000.

[102] European Parliament resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 - 2000/2144(COS)), OJEC C 121/155, 24/04/2001.

[103] See generally J. REIDENBERG, "Privacy Wrongs in Search of Remedies," *Hastings Law Journal*, 2003, vol. 54, pp. 877–898. J. REIDENBERG, "E-Commerce and Trans-Atlantic Privacy", *Houston Law Review*, 2001, vol. 38, pp. 717–749. Y. POULLET, "The Safe Harbor Principles – An Adequate Protection?", paper presented at International Colloquium organized by IFCLA, Paris, 15–16 June 2000, available at: http://www.droit.fundp.ac.be/textes/safeharbor.pdf, last visited 28 February 2004. See also the report prepared in the context of the Safe Harbour revision: J. DHONT, M.V. PEREZ ASINARI and Y. POULLET, with the collaboration of J. REIDENBERG and L. BYGRAVE, *Safe Harbour Decision Implementation Study*, at the request of the European Commission, Internal Market DG, Contract PRS/2003/A0-7002/E/27, not publicly available yet, to be published in DG MARKT website, Data Protection Unit.

[104] When the European Parliament issued its resolution on the draft Commission SH Decision it pointed out : "3. Draws the Commission's attention to the risk that the exchange of letters between the Commission and the US Department of Commerce on the implementation of the 'safe harbour' principles could be interpreted by the European and/or United States judicial authorities as having the substance of an international agreement adopted in breach of Article 300 of the Treaty establishing the European Community and the requirement to seek Parliament's assent (Judgment of the Court of Justice of 9 August 1994: French Republic v. the Commission -- Agreement between the Commission and the United States regarding the application of their competition laws (Case C-327/91))"

European Commission, declaring that the Principles and FAQs annexed therein are considered to ensure an "adequate level of protection".

US organizations adherence to the SH is voluntary. However, if they self-certify to the US Department of Commerce their adherence they are bound by this commitment. They are obliged, then, to comply with the Principles and FAQs to retain the benefits of the SH and to publicly represent that they do so, normally in the form of "Privacy Policies". The SH applies only to sectors which fall under the jurisdiction of the Federal Trade Commission (FTC) or the US Department of Transportation (DoT)[106]. As a consequence, important economic sectors, such as banks, insurance or telecommunications are excluded from the SH framework. Moreover, even if the SH scheme refers explicitly to the human resources data, the jurisdiction of the FTC in this field remains dubious[107]. Then, a US organization can qualify for the SH only if its failure to comply with its commitment to adhere to the SH principles is actionable under the Federal Trade Commission Act section 5 (prohibiting unfair and deceptive acts) or Title 49 United States Code (USC) section 41712. A deceptive practice is defined as a "representation, omission or practice that is likely to mislead reasonable consumers in a material fashion"[108].

The SH Privacy Principles are the following:

- NOTICE: "An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party".
- CHOICE: "An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(2) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice".
  For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was

---

[105] Decisions are one of the sources of Community law. Article 249 TEC, 4th paragraph.

[106] Recital 6 of the Commission Decision.

[107] See J. REIDENBERG "E-commerce and Transatlantic Privacy", *op. cit.*, p. 743

[108] A practice is unfair if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition: see 15 USC section 45(n) and letter of 14 July 2000 from FTC Chairman Mr. Robert Pitofsky to Mr. John Mogg, Director, DG XV, European Commission (set out in the Commission Decision, Annex V).

originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party identifies and treats it as sensitive.

- ONWARD TRANSFER: "To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing".
- SECURITY: "Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction".
- DATA INTEGRITY: "Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current".
- ACCESS: "Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated".
- ENFORCEMENT: "Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations".

Furthermore, the 15 FAQs intend to provide clarification in certain key issues, such as sensitive data, the journalistic exceptions, the role of national DPAs, self-certification, verification, dispute resolution and enforcement, etc.

4.2. Implementation of the Safe Harbour in practise and beyond

Since the adoption of the SH Decision 508[109] companies have adhered. It is not possible to state, *a priori*, if such a number represents a successful story or not. To make an evaluation, it would be necessary to know how many companies conduct flows of personal data from the EU to the US that are not covered by the exceptions of Article 26(1), appropriate or standard contractual clauses, or any other alternative method considered "adequate" by a national DPA.

So far, there has not been any complaint from a data subject or DPA as a consequence of a violation to the SH by a US organization. One could then deduce that the implementation is correct and that all the obligations and rights foreseen in the SH scheme are fully respected by US organizations. Nevertheless, an analysis of the privacy policies content, or even the lack of publicly available privacy policies in certain cases, could demonstrate, to a given extent, the contrary. For instance, if we have a look at the SH list posted on the DoC website[110], we will find cases where a direct access to the privacy policy is not possible. On the contrary, a hyperlink will lead us to the homepage of the US organization that has self-certified to the SH. When at this webpage, it is sometimes difficult to find the link to the privacy policy. After having reached the privacy policy, its terms may be not very clear, or the SH principles may not be all represented. Should we understand that if there is no representation of a SH principle there is no obligation *vis-à-vis* a European data subject? This remains unclear.

Whereas in the EU, the legitimacy of processing activities is structured around the concept of "purpose", the purpose is usually difficult to find in SH privacy policies. Moreover, the DoC self-certification page does not foresee any entry for this specification to be made. This is just another example of the kind of problems that can be found in the implementation practise.

The enforcement mechanisms may present other kind of difficulties, for instance, the sanctions to which US organizations would be subject, if they violate the SH principles, are not always specified in the privacy policies or privacy programmes. The same could be said concerning remedies or the obligation to reverse the effects of breach.

One may wonder, then, if the EU data subject is aware of the transfer of her data to the US, and if so, to what extent she is conscious of the rights foreseen in the SH to protect her against illegitimate processing. One may wonder, also, if US organizations that give evidence of good will by adhering to the SH and that make efforts and invest in the implementation of it into its business practises have a full understanding of a system that is quite different from the one they are used to apply. We could say that, in principle, efforts remain to be made for a full implementation of the SH scheme.

Beyond the SH, we have to (re)consider the scope of EU-US transatlantic cooperation broadly. The SH is just a first step to reach the goals described in the joint political documents. We have seen that its scope of application is restrictive. However, there have not been further efforts to enlarge its scope (at least no official negotiations have started).

4.3. Have there been impediments for a successful cooperation?

[109] As of 8/06/04. Check : http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

[110] http://www.export.gov/safeharbor/

What would be "successful cooperation" in this field? From the perspective of the NTA and the related political documents we have considered, it would be the creation of a legal framework for the effective protection of privacy and personal data that can contribute to the expansion of world trade and closer economic relations.

The SH is, indeed, a fragmented solution both within the framework of the Directive scope of application and the framework of the NTA. It covers only certain economic sectors and within these sectors only the US organizations that self-certify their adherence to the principles. Furthermore, it is limited to the US, not giving an answer to the organizations that work on a multinational basis[111]. We may even wonder if it is a case of "joint governance" or just a unilateral instrument to solve, partly, a legal problem. Thus, the scope of cooperation beyond the SH has been quite limited.

The impediments are rather intrinsic. Privacy is a subject matter that has been regulated differently by both parties, however, certain degree of understanding on common legally-binding standards would benefit the development of the Information Society in general, and of electronic commerce in particular. Here, we are not strictly speaking about trans-border data flows that fall into the Directive's scope of application. The normal use of open networks involves many activities that do not imply the application of Directive 95/46/EC (neither of Article 4.1(c)[112], nor of Article 25(1)).

Could this be the case, for instance, of a simple operation of e-commerce? The buyer (data subject) is located in the EU. The seller (data controller) is located in the US. The seller needs the data subject's personal data to be able to deliver the product. She decides the means and purposes of the processing activity, but, as she is not located in the EU, and she is not making use of equipment located in the EU to process personal data, she is not subject to Directive 95/46/EC.

However, even if the Directive is not applicable, there is a transatlantic political interest that this data be processed in legitimate terms and respecting certain rights of this data subject. If she realizes, for instance, that after the e-commerce operation she starts receiving a lot of unsolicited commercial e-mails she will suspect that her data has been shared or sold. Her consent has not been asked for such use. She reads again the privacy policy posted on the e-commerce site and realizes that the seller has neither made any representation about third parties data sharing, nor about the right of access. As a consequence, the data subject cannot

---

[111] See : Article 29 Personal Data Protection Working Party, *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*, WP74, 3 June 2003.

[112] National law applicable: "1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (...) (c) 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, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself".

sue the seller under the FTC Act. Even if the privacy policy would have made these kind of representations, it will be for the European data subject to scrutinize the content of this privacy policy and to introduce her complaint before a US Court, or before an unknown ADR located in the US, functioning under unusual rules and in a language that is not the one of the European data subject. This individual would be more than disappointed with this transatlantic experience.

The US self-regulatory approach may not give the EU data subject the protection to which she is used to. This can affect, indeed, a more active participation in e-commerce. Even if, in the case of the example, she has decided to provide her data, and this data is necessary for the performance of the contract, she would not like that data to be used for incompatible purposes, sold and integrated into an indeterminate number of different data bases to profile her, considering the type of good she has bought, etc.

"Impediments" for cooperation arise because the protection of privacy and personal data is fostered through different mechanisms by both parties. Indeed, a solution "in the middle" is quite difficult to be reached. Could we blame the EU for not diminishing the protection deserved by a human right? Could we blame the US for not adopting a general privacy law when their national approach to most e-commerce related mattes (including privacy) is market-lead? The SH could be seen as this kind of solution "in the middle". Yet, is it desired to continue in this line, for example, extending the SH to the banking sector? Or, should negotiation stand beyond the Directive and consider that what could be affecting the development of e-commerce and global digital trade are cases that may fall outside the Directive? Could we say that "impediments" for cooperation can be found in the narrow-Article 25(1)-oriented base of negotiation for transatlantic privacy?

4.4. Institutions and practises for overcoming obstacles

The negotiation of the SH has been actively conducted between the European Commission and the US Department of Commerce. Other organisations and bodies have supported those institutions. For instance, the Article 29 Data Protection Working Party[113] has closely followed the evolution of the draft principles and FAQs, guiding the Commission for the achievement of a legitimate framework. The private sector has also participated in this process. Those institutions are to be called again for the improvement of SH implementation.

Within the SH framework, the practise that have been used to overcome the obstacles experienced was the use of co-regulation techniques. The SH principles have been elaborated jointly by the public and the private sector.

4.5. Future steps

Some of the future steps that the US and the EU might undertake, to strengthen cooperation and attain their common NTA goals, can be summarized as follows:

[113] See footnote 101

(a) In the near future,

- Rectify the errors in the implementation of the SH;
- Clarify SH concepts that remain unclear, bearing in mind, that they will be applied by US organizations that are not familiar with the EU Directive;
- Increase EU data subjects and US data controllers awareness of their respective rights and obligations under the SH, a task that has to be conducted by all the institutions with responsibilities and interests in the correct application of this scheme;
- Grant an increasing role and visibility to the SH European Panel[114] in order to assist the European data subjects in addressing their complaints;
- Clarify the statutes and competences of the ADR bodies.

(b) In mid term,

- Enlarge the scope of application of the SH, to cover all the sectors involved in trans-border data flows

Beyond the SH, a closer regard to Privacy Enhancing Technologies (PETs) and the role of technical standards organizations (W3C, IETF[115], ISO, CEN, etc.) has to be encouraged, bearing in mind that they are a "complement" to traditional regulatory choices[116].

Moreover, the adoption of sector specific codes of conduct would motivate the active intervention and compromise of the stakeholders involved. At European level, the Federation of European Direct Marketing (FEDMA) Code of Conduct[117] could be an example of that trend[118]. Further development of Binding Corporate Rules initiatives would be helpful for multinational companies' need[119].

(c) In a longer term,

---

[114] See FAQ 5 and 11 of the SH. The website of the Secretariat of the SH Panel is: http://forum.europa.eu.int/Public/irc/secureida/safeharbor/home

[115] For a description of roles of the W3C (World Wide Web Consortium) and the IETF (Internet Engeneering Task Force) see : J. BERLEUR and Y. POULLET "Quelles régulations pour l'internet?", in *Gouvernance de la Société de l'Information, op. cit.*

[116] See: J. REIDENBERG "*Lex Informatica*: The Formulation of Information Policy Rules through Technology", 76 Texas L. Rev., 1998, pp. 553-584. L. LESSIG, *Code and other laws of Cyberspace*, Basic Books, 1999. J. REINDENBERG, "States and Internet Enforcement", *Ottawa Journal on Law & Technology*, Vol. 1 Issue 1, 2004, pp. 1-25. P. SCHWARTZ "Beyond Lessig's *Code* for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices", *Wisconsin Law Review*, 2000, p. 743-788.

[117] European Code of Practice for the Use of Personal Data in Direct Marketing, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77-annex_en.pdf

[118] See : Article 29 Personal Data Protection Working Party, *Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing*, WP77, 13 June 2003.

[119] See: Article 29 Personal Data Protection Working Party, *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*, WP74, 3 June 2003.

- Signature of an International Agreement containing harmonized personal data protection rules.

Again in the formula "beyond the SH", an international Agreement seems to be a natural recourse to harmonize divergent regulations for a common understanding. However, what would be the framework for such an Agreement? A bilateral instrument seems insufficient. Which international organization would be then called to assume responsibility and act proactively?

The OECD has a restricted membership, and its efforts, even if innovative when adopted, are not being used to solve concrete problems as the ones described herein, because of the "soft law" nature of the Guidelines. The WTO has considered, so far, privacy and data protection as an exception to its rules. Whilst the Doha agenda had foreseen these issues in the context of the e-commerce discussion, no visible result has derived from Cancun in this realm. It is true that the topic will have to be faced, sooner or later, at the WTO. But this will imply another political discussion and choice, including, to what extent the WTO has jurisdiction in a matter that, at least for some members, is a question of human rights? Or, to what extent countries are willing to enlarge WTO competences in this direction? Would they be obliged to do so, not to leave people without human rights protection when a case involving them is decided in this international sphere?[120]

It has to be underlined that an integral approach to privacy is preferable, that is, not considered only as a "barrier" to trade that can be accepted under certain circumstances. Precisely for this reason, the intervention of the UN would be preferable, insofar this institution has to envisage all aspects of the global society not only the economic but also the cultural, social and human rights ones. The UN could be a discussion and decision-making body to be taken more into account, as a way to solve privacy and personal data protection implications of global networks. The UN has adopted the 1990 Guidelines on computerized personal data files. This document reflects broadly accepted fair information principles. In a more general spectrum, Article 12 of the Universal Declaration of Human Rights stipulates that: "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". This makes the UN a legitimized institution to develop a consistent answer to the problematic described herein[121].

5. Concluding remarks

[120] See : E-U PETERSMANN, "Time for Integrating Human Rights into the Law of Worldwide Organizations", *The Jean Monnet Program*, Jean Monnet Working Paper 7/01, available at: http://www.jeanmonnetprogram.org/papers/01/012301.rtf , last visited 20/05/04.

[121] Furthermore, WSIS Declaration of Principles has stated: "20. Governments, as well as private sector, civil society and the *United Nations* and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders", emphasis added.

The early "euphoria" of the new economy revolution called the attention to certain rights of the individual that could remain unbalanced if not properly addressed. The structure of the Internet demonstrated that these intrinsic risks could, as a consequence of threatening individuals' rights, hamper Information Society and e-commerce progress.

The "euphoria" of progress was, due to its influence in EU-US relations, transmitted into the NTA "policy". The EU and the US jointly considered that, in order to contribute to the expansion of world trade and closer economic relations, in particular for the expansion of e-commerce, it was necessary to ensure the effective protection of privacy with regard to the processing of personal data on global information networks.

However, this political agreement has not been fully translated into regulation to guarantee its effectiveness. The way from "policy" to "regulation" has not been completed. Of course, the problem lies between the different conceptions about the type of "regulatory method" needed: State regulation, co-regulation, self-regulation, regulation through technology, and the degree of exclusion or complementarity among them. The point of view of the EU and the US is quite different: European stakeholders are more confident in legislation, administrative actions and criminal sanctions in order to fight against privacy threats. At the same time, we have to consider the scarcity of public awareness and Courts' interventions. This attitude is criticized by certain American stakeholders, asserting that the market, under the pressure of the media and the Human Rights associations will lead to the adoption of appropriate privacy rules. To date, most of the Privacy cases have been developed within US, even if (or "because of"?) there is no comprehensive Privacy Act.

Nevertheless, this is not an issue that can be solved and legitimately decided only by the EU and the US, since the effects have a global impact. Potentially, the absence of a bilateral agreement could give room to a wider dialogue and solution, for instance at the UN level. Notwithstanding, such a wide Agreement would take a remarkable long negotiating period. In the meantime, the US and EU would have to look closer at the NTA and decide if they will continue the same line of action in what concerns privacy and data protection, and if so, they will have to try to reach a degree of consensus for harmonization. Consensus at this bilateral level, would pave the way for broader consensus.

So far, the transatlantic dialogue has been very concentrated on the search for solutions to avoid the application of Article 25(1) of the Directive to the US. A complete view of TBDF scenarios, applicable law and jurisdiction issues can help to have an understanding of other cases that are excluded from the scope of application of Directive 95/46/EC, yet are surrounded by legal uncertainty for the digital market place actors.

Finally, it has to be noted that, after the tragedy of 11 September 2001, many initiatives involving TBDF for security and fight against terrorism issues have taken place. Those initiatives, e.g. the airline passengers' data case, would affect not only the application of Directive 95/46/EC, but also other areas of EU law, like third pillar issues. In the scope of the NTA, it is clear that they exceed the third shared goal, but fall within the second shared goal. Thus, it will be necessary to assess to what extent the scope of privacy negotiations should be broaden also in this direction, bearing in mind that the solution already adopted by the European Commission may encounter certain limitations[122].

[122] Commission Decision of 14 May on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, C(2004) 1914, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/pnr/c-2004-

1914/c-2004-1914_en.pdf. See: see M.V. PEREZ ASINARI and Y. POULLET "The airline passenger data disclosure case...", *op. cit.*. See also, by the same authors, "Airline passenger's data: adoption of an adequacy Decision by the European Commission....", to be published in *Computer Law & Security Report*.