

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### The WTO and the protection of personal data.

Pérez Asinari, María Verónica

*Published in:*  
18th BILETA Conference

*Publication date:*  
2003

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

#### [Link to publication](#)

*Citation for pulished version (HARVARD):*

Pérez Asinari, MV 2003, The WTO and the protection of personal data. Do EU measures fall within GATS exception? Which future data protection within the WTO e-commerce context? in *18th BILETA Conference: Controlling INformation in the Online Environment : April, 2003, QMW, London*. BILETA, pp. 1-9.  
<<http://www.bileta.ac.uk>>

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



**18th BILETA Conference: *Controlling Information in the Online Environment***

*April, 2003  
QMW, London*

## **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?**

María Verónica PEREZ ASINARI  
*University of Namur, Belgium*

### **1. Introduction**

Export of personal data is a business necessity for many information management activities or provision of services in general.<sup>[1]</sup> Information technology stresses this asset, consumers can be easily localised in cyberspace, and they can also be profiled, not only using the data they have consented to provide, but also using unknown traces.

Information exchange reality across boundaries was early analysed in Europe from the perspective of the Internal Market: due to the passing of privacy and data protection laws in different member states, obstacles to the free flow of data could be created due to the disparity of legislation.

Directive 95/46/EC<sup>[2]</sup> was passed in order to harmonise divergent 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 reach the Internal Market's requirement of free flow of personal data.

This legislation can be analysed in the light of the WTO rules since it can affect trade in services. In this paper we will address two main questions connected to the present and future of the protection of privacy and personal data within the WTO context. The approach will be developed from a European perspective.

The General Agreement on Trade in Services (GATS) envisages four types of service supply:

- (a) *from the territory of one Member into the territory of any other Member* (cross-border supply: the possibility for non-resident service suppliers to supply services cross-border into the Member's territory)
- (b) *in the territory of one Member to the service consumer of any other Member* (consumption abroad: the freedom for the Member's residents to purchase services in the territory of another Member)
- (c) *by a service supplier of one Member, through commercial presence in the territory of any other Member* (commercial presence: the opportunities for foreign service suppliers to establish, operate or expand a commercial presence in the Member's territory; such as a branch, agency, or wholly-owned subsidiary)
- (d) *by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member*<sup>[3]</sup> (presence of natural persons: the possibilities offered for the entry and temporary stay in the Member's territory of foreign individuals in order to supply a service)

The first and second case would certainly involve e-commerce examples<sup>[4]</sup>, where trans-border data flows (TBDF) of personal data normally take place. The third case and its implications concerning TBDF could be exemplified by Human Resources information management activities carried out by multinational companies.

### **2. The EU regulation on TBDF**

The Directive prohibits trans-border data flows to countries not giving an adequate protection to personal data (Article 25.1). It also creates several ways for interpretation and methods of derogations of this general rule (Article 25.6, 26.1,

26.2, 26.4).

Article 25.2 states the way “adequacy” should be analysed: *“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.”*

Article 26.1 of the Directive contains a set of derogations to the general rule regulating that Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may take place on condition that (a) the data subject has unambiguously given his consent 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 precontractual 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; etc.

Further, Article 25.6 of the Directive provides that the Commission may find that a third country ensures an “adequate level of protection” by reason of its domestic law or of the international commitments it adheres to, particularly upon conclusion of the negotiations referred to in paragraph 5 of Article 25, for the protection of the private lives and basic freedoms and rights of individuals.

The Directive offers other possibilities to make international transfers possible. Article 26.2 states that a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25.2, where the controller adduces adequate data protection safeguards; such safeguards may in particular result from appropriate contractual clauses. Those safeguards, apart from contracts<sup>[5]</sup>, could, for instance, have the form of Privacy Policies, Codes of Conduct<sup>[6]</sup>, etc. Apart from that, Article 26.4 states that where the Commission decides that certain standard contractual clauses offer sufficient safeguards as required in paragraph 2 of Article 26, member states shall take the necessary measures to comply with the Commission's decision.

This regulatory framework has created a remarkable controversy between the EU and the US in the way to try to find a solution that allows the free flow of personal data, since, namely in the e-commerce sector, the US only envisages data protection regulation through the use of self-regulatory means, what results, in the practise, in a lower standard of protection. After more than two years of negotiations, a *sui generis*<sup>[7]</sup> agreement, known as the “Safe Harbour”<sup>[8]</sup> was adopted by the European Commission. However, the controversy and dialogue have to not finished there<sup>[9]</sup> since this is not an agreement covering all the societal sectors.

The European Commission has also adopted adequacy decisions concerning Hungary<sup>[10]</sup>, Switzerland<sup>[11]</sup> and Canada<sup>[12]</sup> (and it will probably proceed concerning Argentina<sup>[13]</sup> in the near future). The first two cases involve examples of general adequacy findings, implying that the whole legal system offers adequate protection. The third case is a partial recognition, but wider than the Safe Harbor, as it considers that the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act) provides adequate protection only for certain categories of personal data transferred from the EU to Canada (e.g. private sector organisations that collect, use or disclose personal information in the course of commercial activities), and not for the public sector.

From an international trade perspective and considering that the system of trans-border data flows created by the Directive can constitute, in certain circumstances an obstacle to trade, we will analyse whether it would be justified as falling under the exceptions to the application of the WTO rules.

### **3. Regulation by the WTO (or the non-regulation option...) on privacy and data protection [14]**

Article XIV of the General Agreement on Trade in Services (GATS) regulates the “General Exceptions” to the application of its rules. The relevant part for the current study states: *“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: (...); c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (...); (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; (...)”*

For this exception to be valid some conditions have to be fulfilled. There has not been any Panel Decision on Article XIV (c)(ii) yet. An analysis can be conducted, by analogy, on Panel Decisions concerning the exceptions to the application of WTO rules contained in Article XX of the GATT<sup>[15]</sup>, to have a close look at the interpretation given to the conditions.

In those decisions, we can find Panel interpretations on what are the parameters to consider for the application of an exception to the WTO rules, what is the methodology to follow, what are the premises for the use of the “necessity test”,

the meaning of non discriminatory application in the sense of the “chapeau” (introductory clause), etc.

All those concepts have to be assessed in the light of the adequacy method, which is used by the EU data protection legislation to authorize or not data transfers to third countries, both at the theoretical level (Article 25.2 of the Directive, Article 29 DPWP Working Document No. 12, Doctrine) and practical level (Commission Decisions of Adequacy Findings).

This analysis has to be complemented by the Human Rights perspective of privacy and data protection within the EU, and the responsibility of member states as signatories of international binding documents in this realm.<sup>[16]</sup>

Following Panel decisions we could conclude that a “four-step-methodology” has to be followed when assessing the pertinence or not for the use of the exception.

But before using the four-step-methodology, given a concrete case, we will have to analyse whether the country in question has made specific commitments in the service sector under discussion<sup>[17]</sup>, or regarding the “Most-favoured Nation Treatment”, whether the member can maintain a measure inconsistent with it, provided that such a measure is listed in, and meets the condition of, the Annex on Article II Exemptions<sup>[18]</sup>. “It is only by reference to a country’s schedule, and (where relevant) its MFN exemption list, that it can be seen to which services sectors and under what conditions the basic principles of the GATS –market access, national treatment and MFN treatment- apply within that country’s jurisdiction.”<sup>[19]</sup>

Then, the steps are the following:

### **1) First step: determine whether the measure under discussion is inconsistent with a GATS’ provision.**

For example, we need to examine whether the measure under discussion is contrary to the Article II “Most-Favoured-Nation Treatment”, Article VI “Domestic Regulation”, Article VII “Recognition”, etc.

Indeed, a conflict with Article II of the GATS, “Most-favoured Nation Treatment” principle (MFN), could be envisaged as regards the application of the EU privacy and personal data protection legislation (specifically what is foreseen as regards trans-border data flows): “1. *With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country*” (favour one, favour all)<sup>[20]</sup>. Given a benefit to a nation, the refusal to others is only permitted if such treatment is expressly listed in the relevant member’s Annex that sets out its MFN exemption.

We can think about data processing services. Those located in the US, for instance, will receive a different treatment (less favourable) than those located in Switzerland or Hungary, unless they have joined the “Safe Harbor”. This because Article 25.1 of the Directive establishes a prohibition to trans-border data flows to countries not giving an adequate protection to personal data, and Switzerland and Hungary have been declared as countries giving an adequate protection by the European Commission, which result in the free-flow of information, as we have already pointed out above. The “inconsistency” is indeed this prohibition and the possibility to derogate this rule when Adequacy Finding Decisions have been adopted, creating a differentiate treatment among third countries.

The same can be envisaged as regards human resources information management, e-commerce operations, advertising services, market research and public opinion polling services, etc., where the flow of personal data could be subject to certain restrictions.

The examples above can be evaluated also *vis-à-vis* Article VII: “1. *For the purposes of the fulfilment, in whole or in part, of its standards or criteria for the authorization, licensing or certification of services suppliers, and subject to the requirements of paragraph 3, a Member may recognize the education or experience obtained, requirements met, or licenses or certifications granted in a particular country. Such recognition, which may be achieved through harmonization or otherwise, may be based upon an agreement or arrangement with the country concerned or may be accorded autonomously. 2. A member that is party to an agreement or arrangement of the type referred to in paragraph 1, whether existing or future, shall afford adequate opportunity for other interested Members to negotiate their accession to such an agreement or arrangement or to negotiate comparable one with it. (...). 3. A member shall not accord recognition in a manner which would constitute a means of discrimination between countries in the application of its standards or criteria for the authorization, licensing or certification of services suppliers, or a disguised restriction on trade in services.*”

The “criteria for authorization” of service suppliers, can be influenced by Adequacy Decisions or by the level of protection given by a country. The EU have recognised that concerning Switzerland and Hungary data protection “requirements” are “met”. The same opportunity has to be given to other countries, and, again, this opportunity has to be administered in a way that does not constitute a discrimination or a disguised restriction.

The next three steps will help to assess whether this “inconsistency” is justified or not, and whether the use of the

exception to the WTO rules is legitimate.

**2) Second step: evaluate whether “(...) the ‘laws or regulations’ with which compliance is being secured are themselves ‘not inconsistent’ with the General1) Agreement”.**

The “spirit” of the Agreement should thereby be considered in order to assess what represents “consistency” with it. Whereas the first step focuses on a punctual assessment (an specific provision of the Agreement), the second one focuses on a general assessment (the Agreement as a whole). As for the GATS, the reference is the Preamble. There we find an explicit mention highlighting the importance of “*giving due respect to national policy objectives*”, and also the recognition of “*the right of Member States to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives (...)*”.

Having said that, we see that Directive 95/46/EC, which is the regulation with which compliance is being secured by the application of Article 25.1 (as well as the possibility given in Article 25.6), is not inconsistent, in principle, with the Agreement, since the (supranational) policy objectives pursued give the right to the EU to regulate in this realm. The policy objectives, that is the protection of data privacy, are expressed in the European Convention for the Protection of Human Rights and Fundamental Freedoms[21], in the Charter of Fundamental Rights of the European Union[22], and in many National Constitutions[23] of the EU member states.

**3)Third step: evaluate whether the measures are “necessary to secure compliance” with those laws or regulation.**

Panels normally[24] consider that this evaluation should be able to determine whether the State would have an available alternative measure no or less restrictive to trade that could reasonably be expected to employ to achieve the same policy objective and which is not inconsistent with other GATT (or GATS) provisions. If the result of the search is positive, the use of the exception has to be excluded.

The Philosophy of Article 25.1 can be resumed by the fact that within the EU the protection of privacy and personal data is a human right and has been attributed a high level of protection (that should not be loop-holed by transferring data outside the EU). That is why the Directive creates rights for the data subject, duties for the data controller, liability, remedies, sanctions, independent data protection authorities, etc. Outside the EU the situation is not always similar, there are countries providing a high level of protection, countries providing for less protection, countries with different legal conceptions (so it is necessary to analyse what the result of this regulation is in terms of “adequacy” ), and countries with no protection.[25]

The rule on TBDF has been created due to the easiness to send data to countries providing for no or less protection, (easiness that has been increased by the use of information technologies), in order to circumvent EU law and carry out processing activities that are forbidden in the EU.

However, the Directive provides for derogations (see *supra*) to this principle, facilitating data flows while preserving data protection rights, as well as preventing State liability for non compliance with internationally binding human rights instruments[26].

The outcome of the “necessity test” would be positive if, after having analysed whether any of the alternative solutions provided to allow data transfers, none of them could be used. In this case, the prohibition would be, in principle, “necessary” to assure compliance with the Directive.

**4) Fourth step: assess whether the measures are “not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade”.**

A “discrimination” would be “arbitrary or unjustified” if the EU, or the Member States, when applying the law to a concrete case, would allow the transfer of personal data to one country and forbid it, under the same circumstances, to another one, alleging that it does not present an “adequate protection”, given the situation that both countries have similar regulations, or present the same lack of regulation in an specific sector, for example, the private one.

A “disguised restriction” is a sophisticated barrier to international commerce. It is a burden coming from the legal or administrative framework, which reason to exists is not necessary or weak, and is funded on protectionism. It can take place, for instance, in case the analysis of a third country data protection regime is not well founded in terms of the effective protection given to personal data, and only looks for giving privileges to European service providers.

For the evaluation of third countries adequacy, the Article 29 Working Party has issued several documents describing the methodology to follow in the assessment to be made.[27] They have described what are the principles of content and procedure that has to be present in a third country to be considered “adequate”. We have to bear in mind that this methodology has to be applied under a case-by-case, flexible, pragmatic and functional approach[28], in order to respect other country’s legislation in particular, and legal systems in general, as well as different regulatory instruments (self-regulatory or co-regulatory).



In this step, the exception would fail if given the same conditions (same level of protection) one country is considered to provide for an adequate level and the other not. Indeed, given the characteristics of the “adequacy method”, the risks of arbitrary or unjustifiable discrimination are reduced, compared to the results that would arise from the use of the “equivalence method”[29]. However, the adequacy method consists in a subjective analysis, so there is a certain risk that it could be used in a discriminatory way if not properly applied. This fact can only be analysed in a concrete case, and not *in abstracto*.

#### **4. Which future for privacy and data protection within the WTO e-commerce context?**

The world trade system has to face new challenges for regulation due to the e-commerce revolution. If we think about the very principles, they are the same..., the exchange of goods and services is a matter of human nature. However, even if the “essence” has not changed, the means are new, and they pose questions concerning the interpretation of former rules *vis-à-vis* new realities, as well as the necessity or not of passing new rules.

The World Trade Organisation (WTO) is the global international organization dealing with the rules of trade between nations. It has been created by the Uruguay Round negotiations (1986-94), and it is the successor of the GATT.

The WTO’ highest decision-making body is the Ministerial Conference.[30] The declaration on global electronic commerce adopted by the Second Ministerial Conference (Geneva) on 20 May 1998 had urged the WTO General Council to establish a comprehensive work programme to examine all trade-related issues arising from global electronic commerce.

Accordingly, during the Fourth WTO Ministerial Conference, held in Doha, Qatar from 9 to 14 November 2001, a declaration[31] was issued providing the mandate for negotiations on a range of subjects, and other work including twenty one other issues. One of them is electronic commerce.

##### **4.1 State of negotiations. The Council for Trade in Services**

The Doha Declaration endorses the work already done and instructs the General Council to consider the most appropriate institutional arrangements for handling the work programme, and to report on further progress to the Fifth Ministerial Conference.[32]

Within this set of trade-related issues arising from global electronic commerce, the protection of data privacy is one of the topics that the Council for Trade in Services shall examine and report on.

This will involve, at least from a European point of view, that the Council for Trade in Services will have to examine a question that is considered to be a Fundamental Right.[33] It is known that the WTO has been strongly questioned for not paying enough attention to non-classical-trade issues connected to or involved in the development of economic issues.[34] The Doha Declaration has reaffirmed the importance of paying attention to non-trade issues, for instance, the protection of the environment, the promotion of a sustainable development, the safeguarding of core labour standards, etc.[35]

In the current state of discussions, the protection of data privacy has not taken an important place in WTO public available documents.[36]

However, we need to assess the legitimacy or competence of the WTO to intervene in the regulation of privacy and data protection. The creation of exceptions, as those of article XX of the GATT or of article XIV of the GATS, is a way to “not regulate”.

The competence of the EU (EEC at that time) on the subject matter was severely discussed. Indeed, this was one of the reasons for twenty years of delay between the time when the necessity of a Directive harmonising data protection legislation was acknowledged in the EU, and the date of effective adoption of the instrument. The legal basis was the main point of controversy. How could the EU (EEC) regulate on a fundamental right if it had no competence in this realm? How could the EU (EEC) not harmonise data protection national laws if the discrepancies’ interference with the Internal Market was obvious?[37]

Even if, as the time went by, the EU expanded the reference and competence on fundamental rights, the Directive was passed using as legal basis ex-article 100A[38] (which is the one prescribed to regulate internal market issues). The EU internal market implications were solved harmonising the effective protection given by member states to personal data, in order to permit the free-flow of information.

Could we envisage this sort of evolution at the WTO level? Would this be possible? Would this be desirable? One of the main differences is the nature of “integration” of both institutions, whereas the EU is a “supranational” process, which implies delegation of sovereignty, the WTO is an “intergovernmental” process, with very limited political integration. That is why it is unlikely that, at least with this institutional characteristics, the WTO will evolve in this sense, since

certain governments will be reluctant to globally harmonise a field with, for them, fundamental rights implications in the context of an organization which aim is not the protection of fundamental rights.

#### **4.2 Potential regulation of personal data protection in the context of the WTO?**

It is clear that global norms for privacy would solve many problems. However a simple solution would be very difficult to achieve since data privacy is one of the fields of law where social, historical, and cultural background is more remarkable. [39]

The WTO has not been considered extensively by the doctrine as a possible way to regulate privacy globally, may be because it is difficult to associate the WTO with human rights.

Reidenberg has suggested the adoption of a "General Agreement on Information Privacy" (GAIP) in the context of the WTO[40] considering that the WTO' mission covers e-commerce and can be used to facilitate the protection of citizens within the trans-border data flows. He refers to the experience in the field of intellectual property rights, where substantive standards were passed, which have to be incorporated by each signatory party in its domestic law. However, he points out[41] that "[t]he risk of placing GAIP within the WTO trade framework is that the WTO has an inherent bias toward liberal, market norms; GATT and the WTO are founded on the principle of free trade and market economies".

The author concludes that the significance of such an Agreement is, nevertheless, twofold. "First, the WTO framework offers an institutional process with wide membership. Second, while the institution leans toward market-based norms, the incorporation of GAIP within the WTO along with other non-economic values will transplant social-protection norms to the trade arena. In effect, this transplantation will promote convergence of governance norms." [42]

Swire and Litan also suggest that "[t]he WTO could (...) provide an international forum for harmonising the legal treatment for privacy protection." [43] However, with a different view than Reidenberg, they conclude that one of the disadvantages in using the WTO as a forum for negotiating future data privacy rules is that "negotiations in the WTO are at least as hard to predict as a WTO decision in a particular case. They might result in relatively market-oriented rules. The United States and most developing countries do not have comprehensive privacy laws, so most WTO members have reasons not to agree to European-style privacy laws. But the European Union and some other major countries do have national laws that are stricter than those in the United States. For that reason, negotiations could result in a more law-centered emphasis that the United States, with its emphasis on self-regulation, would prefer." [44]

For the time being, it seems that, apart from questioning the legitimacy or competence of the WTO on personal data protection issues, the US-EU controversy could be installed in the WTO arena if any initiative to regulate this field would be taken. For the moment, the WTO has not proved to be the best place to protect non-trade interests. Actually, we would question the appropriateness of conceiving global governance in such a sectoral and compartmented way that has so many difficulties in coping with trans-sectoral issues. However, the will expressed by Reidenberg as a second significance is strongly shared by us, since an economic integration process that does not pay attention to social-protection norms, is simply "not sustainable".

#### **5. Concluding remarks**

The WTO rules set for the right of member states to regulate public policy objectives. One example is the adoption of measures for the protection of personal data. In the case of the EU, the requisites asked for in the necessity test and the "chapeau" are covered, in principle, by the adequacy finding methodology. This would involve, however, a case-by-case analysis.

The "four-steps-methodology" can result in the legitimate use by the European Union of the exception foreseen in Article XIV (c) (ii) to regulate trans-border data flows in order to protect privacy and data protection under the scope of application of the Directive 95/46/EC. A grey area could be found in adequacy finding proceedings if not applied properly or equally to the evaluation of third countries regimes, which could fall outside the requirements of the "chapeau".

E-commerce is a domain where personal data protection has to be addressed properly due to the risks that the misuse of it represents (from a consumer perspective: violation of his fundamental rights; and from a business perspective: endanger of trust and confidence in the e-commerce market place). Certain degree of global consensus could facilitate on-line personal data flows. However, and being realistic, this is a realm full of controversies and political discussions. So, the absence of consensus will continue giving the EU the right to use the exception of the GATS (provided all the requisites are fulfilled in the particular case).

\*I would like to thank Jan Dhont, researcher at the CRID, for his valuable comments on this paper.

\*\* This study was prepared in the context of the project “Privacy: Human Liberty or Consumer Right? The EU-US Debate”, Fonds Spécial de Recherche (F.S.R.) – FUNDP-, Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium. The project is directed by Prof. Yves Poullet.

- [1] C. HAMELINK “Transnational Data Flows in the Information Age”, *Studentlitteratur, Chartwell-Bratt Ltd.*, The Netherlands, 1984. J. BING “Data Protection in Practise. International Service Bureau and Transnational data Flows”, *Universitetsforlaget AS*, Oslo, 1985. R. WELLINGTON BROWN “Economic and Trade Related Aspects of transborder Data Flows: Elements of a Code for Transnational Commerce”, *Studentlitteratur, Chartwell-Bratt Ltd.*, Sweden, 1986. X, “Freedom of Data Flows and EEC Law”, Proceedings of 2nd CELIM Conference, Kluwer Law and Taxation Publishers, The Netherlands, 1988. J. REIDENBERG “Resolving Conflicting International Data Privacy Rules in Cyberspace”, *Stanford Law Review*, Vol. 52, May 2000. J. REIDENBERG “E-Commerce and Trans-Atlantic Privacy”, 38 *Houston L. Rev.* 717, 2001, available at: [http://reidenberg.home.sprynet.com/Transatlantic\\_Privacy.pdf](http://reidenberg.home.sprynet.com/Transatlantic_Privacy.pdf). Y. POULLET, S. LOUVEAUX, and M.V. PEREZ ASINARI “Data Protection and privacy in Global Networks: A European Approach...”, *The EDI Law Review* 8: 147-196, Kluwer Law International, The Netherlands, 2001.
- [2] 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 official Journal L 281, 23/11/1995 P. 0031 – 0050. Hereinafter: “the Directive”.
- [3] The part in italics correspond to the text of Article I.2 of the GATS
- [4] In this paper we do not address the issue of whether e-commerce activities should fall under the GATT or GATS, or even if they should need a new type of regulation. The topic has been largely debated. See: (even before the Uruguay Round) R. WELLINGTON BROWN “Economic and Trade Related Aspects of transborder Data Flows: Elements of a Code for Transnational Commerce”, *Studentlitteratur, Chartwell-Bratt Ltd.*, Sweden, 1986. “Communication from the European Communities and their Member States: Electronic Commerce Work Programme” and related documents of 30 November 2000; 17 November 2000; 10 May 2000; 30 July 1999; 27 July 1999; 15 July 1999; March 1999 (1st, 2nd, and 3rd Communication, and Communication on “Scope and Classification Issues”); 25 September 1998. Available at: <http://europa.eu.int/comm/trade/services/ecommerce/contrib.htm>, last visited 25/03/03. M. BACCHETTA, P. LOW, A. MATTOO, L. SCHUKNECHT, H. WAGER, M. WEHRENS “Electronic Commerce and the role of the WTO”, *World Trade Organization*, 1998.
- [5] Article 29 Data Protection Working Party “Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries”, 22 April 1998, WP 9, available at: [http://www.europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp9en.htm](http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp9en.htm)
- [6] Article 29 Data Protection Working Party “Working Document: Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?”, 14 January 1998, WP 7, available at: [http://www.europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp7en.htm](http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp7en.htm)
- [7] We use the term “sui generis” because of it’s special nature, since it does not declare that the whole US system is “adequate” but just the adhesion, by US companies, to the Agreement’ principles and FAQs. See: Y. POULLET “The ‘Safe Harbor Principles’ : An Adequate Protection ?”, *International Colloquium organised by IFCLA*, Paris, 15-16 June, 2000, available at: <http://www.droit.fundp.ac.be/crid.htm>. J. REIDENBERG “E-commerce and ...”, *op. cit.* J. DHONT and M.V. PEREZ ASINARI “New Physics and the Law. A Comparative Approach to the EU and US Privacy and Data Protection Regulation. Looking for Adequate Protection”, to be published in *L’utilisation de la méthode comparative en droit Européen – Usage of Comparative methodology in European law*, Presse Universitaire de Namur, 2003.
- [8] Commission Decision 2000/520/EC of 26.7.2000 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 - Official Journal L 215/7 of 25.8.2000, available at: [http://www.europa.eu.int/comm/internal\\_market/en/dataprot/adequacy/dec2000520ec.pdf](http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/dec2000520ec.pdf).
- [9] See, for instance, *Joint EU-US statement on the transmission of APIS/PNR data from airlines to the United States*, 6 March 2003, available at: [http://www.europa.eu.int/comm/internal\\_market/privacy/docs/adequacy/declaration\\_en.pdf](http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/declaration_en.pdf)
- [10] 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.
- [11] 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.
- [12] 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 of 4/01/2002.
- [13] Article 29 Data Protection Working Party, Opinion 4/2002 on the level of protection of personal data in Argentina. Adopted on 3 October 2002. WP 63, available at: [http://www.europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp63\\_en.pdf](http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp63_en.pdf)
- [14] This part is based in the article M.V. PEREZ ASINARI “Is there any Room for Privacy and Data Protection within the WTO Rules?”, to be published in *The Electronic Communications Law Review*, Kluwer, The Netherlands, 2003.
- [15] Some of this Dispute Settlement Decisions examined are: “United States – Section 337 of the Tariff Act of 1930”,



“Thailand – Restrictions on Importation of and Internal Taxes on Cigarettes”, -“United States – Standards for Reformulated and Conventional Gasoline”, “Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef”, - “United States – Import Prohibition of Certain Shrimp and Shrimp Products”, etc.

[16] Y. POULLET “Pour une justification des articles 4, 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données”, drafted for the *Data Protection Conference on the Implementation of the Data Protection Directive*, Brussels, September 30 – October 1, 2002.

[17] The schedules are documents in which each country identifies the service sectors to which it will apply the market access and national treatment obligations of the GATS and any exceptions from those obligations it maintains. The commitments and limitations are in every case entered with respect to each of the four modes of supply. See: GATS, Part III, “Specific Commitments”. World Trade Organization “Services Sectoral Classification List”, MTN.GNS/W/120, 10 July 1991. For instance see the “Schedule of Specific Commitments” made by the European Communities and their Member States in the Telecommunications Services Sector, World Trade GATS/SC/31/Suppl.3, 11 April 1997.

[18] GATS, Article II.2. It has to be noted that it is not required to specify measures providing for preferential liberalization of trade in services among members of economic integration processes, provided that the conditions described in Article V of the GATS are met.

[19] World Trade Organization “Guide to reading the GATS schedules of specific commitments and the list of article II (MFN) exemptions”, available at [http://www.wto.org/english/tratop\\_e/serv\\_e/guide1\\_e.htm](http://www.wto.org/english/tratop_e/serv_e/guide1_e.htm)

[20] “When GATS came into force, a number of countries already had preferential agreements in services that they has signed with trading partners, either bilaterally or in small groups. WTO members felt it was necessary to maintain these preferences temporarily. They gave themselves the right to continue giving more favourable treatment to particular countries in particular service activities by listing ‘MFN exemptions’ alongside their first sets of commitments. In order to protect the general MFN principle, the exemptions could only be made once; nothing can be added to the lists.” World Trade Organization “The agreements. Services: rules for growth and investment”, available at [http://www.wto.org/english/thewto\\_e/whatis\\_e/tif\\_e/agrm5\\_e.htm](http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm5_e.htm) (last visited 07/04/03).

[21] See : D. YERNAULT “L’efficacité de la Convention Européenne des Droits de l’homme pour contester le système ‘Echelon’ ”, in *Sénat et Chambre des Représentants de Belgique, Rapport sur l’existence éventuelle d’un réseau d’interception des communications, nommé ‘Echelon’*, 25 Février 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. L. BYGRAVE “Data protection Pursuant to the Right to Privacy in Human Rights Treaties”, *International Journal of Law and Information Technology*, vol. 6 no. 3. This paper examines the extent to which the basic principles of data protection laws may be read into provisions in human rights treaties proclaiming a right to privacy. In our opinion, it is important to bear in mind that data protection principles have a double relationship with the right to privacy. It is included in it to the extent that the data can be considered as affecting the private and family life, home or correspondence of a person, and also goes beyond it because non compliance with data protection rules can affect other fundamental rights recognised in the European Convention for the Protection of Human Rights and Fundamental Freedoms, for instance, Right to a fair trial (Article 6), Freedom of thought conscience and religion (Article 9), Freedom of expression (Article 10), Freedom of assembly and association (Article 11), and Prohibition of discrimination (Article 14). Further, Prof. Poulet considers that the notion of freedom viewed as a self-controlled “self-determination” exercised by individuals seems to enlighten the debate and solutions around Data Protection. Y. POULLET “Data Protection between Property and Liberties. A Civil Law Approach”, in *Amongst Friends in Computers and Law*, H. KASPERSEN and A. OSKAMP (ed.), Kluwer, The Netherlands, 1990.

[22] Article 8.

[23] See, for instance, the National Constitutions of Spain, Portugal, Belgium, The Netherlands.

[24] This reasoning has been followed in “United States – Section 337 of the Tariff Act of 1930”, and “Thailand – Restrictions on Importation of and Internal Taxes on Cigarettes”, but not in “Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef”.

[25] Y. POULLET, S. LOUVEAUX, and M.V. PEREZ ASINARI “Data Protection and privacy in Global Networks...”, *op. cit.* J. DHONT and M.V. PEREZ ASINARI “New Physics and the Law...”, *op. cit.*

[26] D. YERNAULT “L’efficacité...”, *op. cit.*

[27] Article 29 Data Protection Working Party “Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy”, 26 June 1997, WP 4, available at: [http://www.europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp4en.htm](http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp4en.htm)

- Article 29 Data Protection Working Party “Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive”, 24 July 1998, WP 12, available at: [http://www.europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp12en.htm](http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm)

[28] See : Y. POULLET, B. HAVELANGE, A. LEFEBVRE, MH. BOULANGER, H. BURKERT, and C. De TERWANGNE “Elaboration d’une méthodologie pour évaluer l’adéquation du niveau de protection es personnes physiques à l’égard du traitement de données à caractère personnel”, *Centre de Recherches Informatique et Droit* (CRID). Commission Européenne – DG XV, Contrat ETD/95/B5-3000/165, Décembre 1996.

[29] This is the method followed in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no.: 108, Strasbourg 28/01/1981, available at: <http://conventions.coe.int/treaty/en/Treaties/Html/108.htm>

[30] The Ministerial Conference brings together all members of the WTO, all of which are countries or customs unions.

The Ministerial Conference can take decisions on all matters under any of the multilateral trade agreements. See: *Ministerial Conferences on the WTO website*, available at: [http://www.wto.org/english/thewto\\_e/minist\\_e/minist\\_e.htm](http://www.wto.org/english/thewto_e/minist_e/minist_e.htm) (last visited 03-03-03). The organisational structure of the WTO, beyond the Ministerial Conference, can be resumed as follows: "(...) The day-to-day work is carried out by the General Council which also convenes as the Dispute Settlement Body and the Trade Policy Review Body. The General Council delegates responsibility to three other major bodies –the Council for Trade in Goods, the Council for Trade Related Aspects of Intellectual Property Rights, and the Council for trade in Services [which is charged with facilitating the operation of the general Agreement on Trade in Services (GATS) and furthering its objectives]. In addition, there are three other bodies which report to the General Council: the Committee on Trade and Development; the Committee on Balance of payments; and the Committee on Budget, Finance and Administration. The director-general, who is appointed by the Ministerial Conference, is also involved in the work of the General Council." P. DAILLIER and A. PELLET "Droit International Public", *L.G.D.J.*, Paris, 1999. C. KOENIG and J-D. BRAUN "The International Regulatory Framework of EC Telecommunications Law: The law of the WTO and the ITU as a Yardstick for EC Law", in *EC Competition and Telecommunications Law*, Kluwer Law International, The Netherlands, 2002, p. 5.

[31] World Trade Organization "WTO Ministerial declaration Adopted on 14 November 2001", available at [http://www.wto.org/english/thewto\\_e/minist\\_e/min01\\_e/mindecl\\_e.htm](http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htm) (last visited 03-03-03)

[32] See: World Trade Organization "The Doha Declaration explained", available at: [http://www.wto.org/english/tratop\\_e/dda\\_e/dohaexplained\\_e.htm#electroniccommerce](http://www.wto.org/english/tratop_e/dda_e/dohaexplained_e.htm#electroniccommerce) (last visited 03-03-03)

[33] Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, available at: <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>.

Article 7 and 8 of the *Charter of fundamental Rights of the European Union*, OJEC C 364/1, 18/12/200, available at : [http://europa.eu.int/comm/justice\\_home/unit/charte/pdf/texte\\_en.pdf](http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf)

[34] "The Seattle talks re-emphasised tensions between WTO rules and international conventions and treaties on human rights and the environment. WTO Members should consider how best to ensure that WTO rules contribute to other international commitments such as the 2015 human development targets. This may require: reforming the WTO mandate to make explicit that trade is not an end in itself; more effective coordination between the WTO and other international institutions; establishing mechanisms to improve understanding of the linkages between international trade policy and equally important non-trade objectives (...); establishing mechanisms to monitor the poverty impact of WTO sanctions." in: OXFAM GB Discussion Paper *Institutional Reform of the WTO*, March 2000, p. ii. J. STIGLITZ "El malestar en la globalización", *Ed. Taurus*, Argentina, 2002, p. 338-341. D. ESTY "The World Trade Organization's legitimacy crisis", *World Trade Review*, UK, 2002.

[35] World Trade Organization "Doha Ministerial Declaration", available at [http://www.wto.org/english/thewto\\_e/minist\\_e/min01\\_e/mindecl\\_e.htm](http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htm)

[36] World Trade Organization "Third Dedicated Discussion on Electronic Commerce under the Auspices of the General Council on 25 October 2002", Summary by the Secretariat of Issues Raised, WT/GC/W/486, 4 December 2002. World Trade Organization "Second Dedicated Discussion on Electronic Commerce under the Auspices of the General Council on 6 May 2002", Summary by the Secretariat of Issues Raised, WT/GC/W/475, 20 June 2002. World Trade Organization "Dedicated Discussion on Electronic Commerce under the Auspices of the General Council on 15 June 2001", Summary by the Secretariat of Issues Raised, WT/GC/W/436, 6 July 2001.

[37] "In international circles, concern about the potential effect of automatic data processing upon the right to privacy began to grow during the late 1960s and early 1970s. But the eventual drafting of international measures specifically for the purpose of protecting privacy interests against the possible misuse of information by automatic means was carried out entirely by regional institutions, mostly European ones. Although the relatively rapid grow of this activity in data protection was deliberately directed at protecting one aspect of personal privacy, it is very unlikely that it would have grown so rapidly had it not been for a quite unexpected economic aspect. Some countries, especially those committed by treaty to reducing tariff barriers, began to fear that others might use their national data protection laws as non-tariff trade barriers. The development of international standards would not only establish minimum requirements for national legislation, but it could also be used to create a community of countries which met those requirements and which agreed on a free market of information among themselves, to the potential exclusion of others." J. MICHAEL *Privacy and Human Rights. An International and Comparative study, with special reference to developments in information technology*, Ed. Datmouth, Unesco Publishing, Great Britain, 1994.

[38] Currently Article 95 TCE.

[39] See: J. DHONT and M.V. PEREZ ASINARI "New Physics and the Law...", *op. cit.*

[40] J. REIDENBERG "E-commerce and ...", *op. cit.*

[41] J. REIDENBERG "Resolving Conflicting...", *op. cit.*, p. 1365.

[42] J. REIDENBERG "Resolving Conflicting...", *op. cit.*, p. 1366

[43] 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. 194.

[44] P. SWIRE and R. LITAN "None of your business. ...", *op. cit.*, p. 195.