New Physics and the law

Dhont, Jan; Pérez Asinari, María Veroníca

Published in:
L'utilisation de la méthode comparative en droit européen = Usage of methodology in European Law

Publication date:
2003

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

New Physics and the Law. A Comparative Approach to the EU and US Privacy and Data Protection Regulation

Jan DHONT and María Verónica PÉREZ ASINARI
CRID

Résumé :

En passant par l'aiguillon de l'organisation des marchés, l'article qui suit traite de l'impact des nouvelles technologies sur les systèmes juridiques existants. C'est surtout la question de la protection des données à caractère personnel qui est mise en avant. À ce titre, l'article met en exergue l'importance du droit comparé dans le transfert de données à caractère personnel entre l'Union européenne et les États-Unis. Les fortes tensions qui traversent les relations juridiques (et politiques) entre l'Union européenne et les États-Unis sont à cet égard emblématiques : la raison de ces tensions tient principalement à la régulation européenne sur les flux transfrontaliers. En effet, la directive européenne admet le transfert de données à caractère personnel à destination des États tiers seulement dans la mesure où ces États offrent un niveau de protection adéquate. Aux fins d'effectuer la comparaison entre les règles européennes et celles des États tiers, la méthode de l'adéquation implique une analyse au cas par cas, flexible, pragmatique et fonctionnelle.

I. Introduction

The global market place is an interesting topic for the comparative scholar. It constitutes a meeting point for social and political actors from different countries, and as a consequence, is an ideal environment to compare different legal systems in order to regulate situations ruled by different legal traditions.

The Internet has brought along new modes of communication and social interaction. Today, European citizens may buy in virtual shops, transact with persons located abroad, follow courses, work, etc., without having to leave the computer-room. With new technologies, the entire world has become reachable from behind the computer screen. With the contraction of space logically comes the contraction of time : transactions can be done non-stop, and with an ever increasing speed. These « new physics » have an important impact on the basic assumptions that ground modern law.

The Internet has created opportunities of communication unknown before. It provides a host of tools and possibilities to individuals, associations, and businesses since it technically allows one-to-all, as well as one-to-one communication. The Internet marks a means of cultural exchange that is different from collective media such as the radio or TV, since it allows individuals to participate and contribute actively to that exchange.

Businesses have also explored the potentials of the Internet to broaden their markets; e-commerce, e-music, e-books, e-conferences, etc., are notions with which most people are acquainted nowadays. Enterprises soon understood that the new digital medium offers powerful means to reach customers. Indeed, the technology behind the Internet helps businesses reach customers individually.

The Internet has produced novel forms of marketing. Internet technology allows the hidden or overt collection of personal data to directly inform individuals on (new) products/services. Data-mining techniques enable businesses to determine the personal interests of individuals, and to adjust advertising to their personal interests. It has become clear that the Internet enhances customer choice, but this has not come for free : individuals may often pay with their personal data. The economic value of personal information fluctuates over time, and is a function of different complex parameters. The cost of data collection and processing in an online environment is relatively low. Furthermore, it is an inherent characteristic of the Internet that it generates information on communications (e.g. traffic data[1]). Such information can be useful for marketers to determine individuals' interests and to develop more efficient marketing techniques to bring the right information to the right person[2]. However, this evidently creates privacy risks.

The Internet has also produced new forms of human resources information management, facilities for medical and pharmaceutical research data exchange, tourism reservation management, credit card information management, etc. These different global services are carried

1. Article 2(b) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O.J.*, n° L 201, 31 July 2002.
2. See Erika S. KOSTER, « *Zero Privacy : Personal Data on the Internet* », available at : http://www.oppenheimer.com/introprop/news/zeroprivacy.html, (last visited : 22/07/02).

out via the same electronic medium, and from the perspective of data protection, do not constitute different worlds.

Should legislatures intervene to prevent risks inherent in data processing, or does the market offer sufficient protection ? The solutions given in the EU and the US to regulate privacy, mainly *vis-à-vis* the Internet and e-commerce, present a different approach. Comparisons of both systems are often made, since the US is Europe's most important commercial partner, and many personal data flows are conducted in the context of businesses' information management .

This article develops one aspect of the impact that the new market place has on legal systems : privacy and data protection. It explains the importance of comparative law when dealing with transfers of personal data between the EU and the US. It focuses on the processing of personal data in the private sector. It argues that with the proliferation of new technologies, such as communication over the Internet and networks, comparative law is a practical need to provide adequate protection of fundamental rights and consumer rights.

II. Practical Need of the Comparative Method

The basic legal instrument in the field of personal data protection and privacy in the European Union is Directive 95/46/EC[3]. This Directive constitutes a framework directive that sets forth the general principles and rules with regard to the processing of personal data[4]. The Directive contains specific provisions on the transfer of personal data to third countries. These transfer provisions are of particular interest to the comparative law discipline since they require that an analysis of the law be made in the country where the data is imported to assess whether the data to be transfered will be protected. The Directive requires an « adequate » level of protection in the country of

3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal*, L 281, 23/11/1995. Hereinafter : « the Directive ». Directive 97/66/EC regulates the processing of personal data and the protection of privacy in the telecommunications sector (to be replaced by Directive 2002/58/EC).
4. For a general introduction, *cf.* Marie-Hélène BOULANGER, Cécile de TERWANGNE, Thierry LEONARD, Sophie LOUVEAUX, Damien MOREAU, and Yves POULLET, *« La Protection des données à caractère personnel en Droit communautaire »*, *Journal des Tribunaux Droit Européen*, June 1997, page 1 *et seq.*

reception of the personal data. Assessing the adequacy entails more than merely juxtaposing laws ; it requires a sound comparative law methodology.

2.1. A General Overview of Directive 95/46/EC

The aims of the Directive are twofold : first, to permit the free flow of personal data between EU Member States, and second, to protect informational privacy and the fundamental freedoms of the data subjects. At the moment of its conception and adoption, the Directive served primarily an economic purpose. Some Member States such as Sweden, France, the UK and some Länder of Germany had personal data protection laws in place that could constitute *de facto* trade barriers. By requiring equivalent protection in the various EU Member States, the Directive aimed to remove the potential obstacles to intra-Community data flows.

Indeed, the Directive is an Internal Market Directive, based on ex-Article 100A (now Article 95) of the EC Treaty. This implies that EU Member States can *in principle* not provide for stricter data protection principles, since this would constitute an impediment to trade[5]. However, the Directive also sets a minimum level of protection. It is not allowed, for EU Member States to lower the level of data protection. During the drafting of the Directive, the countries that already had legislation in place, intended to maintain their national level of protection. Those countries, mainly Germany and France, wanted the level of protection of their domestic data protection regulations to become the European standard.

The Directive's second purpose is to protect fundamental rights and freedoms of persons, in particular the right to privacy with respect to the processing of personal data[6]. The right to privacy is further recognised by the European Human Rights Convention, the EU Charter on fundamental rights, and the constitutions of various Member States. The approximation of these laws could therefore, as indicated above,

5. The Member States can provide for stricter data protection rules, only if (1) the text of the Directives explicitly allows so, (2) the Member States want to maintain a stricter rule and comply with the conditions set forth in Article 95 of the Treaty, (3) the Member States have compelling public interests as set forth in Article 28 of the Treaty, and (4) the fundamental principles of the Treaty are respected.

6. Article 1 of Directive 95/46/EC.

not lead to any lessening of the level of protection[7].The Directive does not provide a definition of privacy. It sets forth principles and rules on the processing of personal data. It mainly limits the use of personal data so as to avoid that this data may (even potentially) be used to restrict individuals' freedoms. The underlying idea is that informational privacy is essential to protect citizens against discriminatory or other harmful decision-making based on personal data.

The Directive concerns personal data pertaining to natural persons (not those of legal persons)[8]. Its requirements are not specific to a certain socio-economic sector ; it lays down cross-sectoral principles. The reasons why framework legislation was devised include *inter alia* : (1) the difficulty to anticipate what data uses are harmful and what data uses are not ; (2) provide for preventive means of protection ; (3) anticipate privacy risks resulting from the cross-sectoral flow of personal data ; and (4) the assumption that informational privacy is a fundamental right and therefore the exclusion of certain sectors is not justified. Both the public and private sector are subject to the Directive's requirements[9].

Processing of personal data is subject to general principles which aim at offering transparency in data processing, minimum control for the data subject, and restriction of processing. The data controller, i.e. the natural or legal person that decides on the purposes and means of a data processing, must process the personal data fairly and lawfully, and for explicit and *legitimate purposes*[10].

Determination of the exact purpose of the data processing is crucial because it is an important point of reference to assess the legality of the processing. For instance, personal data may not be processed for purposes that are incompatible with the initial purposes of the processing, and must be adequate, relevant and not excessive in relation to those purposes. Also, the quality of the data processing is gauged by reference to its purposes : personal data must be accurate and, updated for the intended purposes. In addition, personal data may be

7. See Recital 10 of the Directive.

8. However, Directive 2002/58/EC protects the « legitimate interests of legal persons » also.

9. It must be noted that Article 13(1) of the Directive provides for exemptions and restrictions with regard to the processing of personal data for certain public purposes, such as national security, defence, public security, etc.

10. Article 6 of the Directive.

processed, only in the presence of a legitimate basis, such as (1) the data subject's unambiguously given consent, (2) the processing being required for the performance of a contract to which the data subject is party, (3) the processing being necessary for compliance with a legal obligation to which the controller is subject, (4) the processing being necessary in order to protect the data subject's vital interests, (5) the processing being necessary for the performance of a task carried out in the public interest, and (6) the processing being necessary for the purposes of the legitimate interests pursued by the controller or by athird party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject [...][11].

This last legitimacy ground seems to create a virtually unlimited ground for the processing of personal data. The ultimate conceptualisation of « fundamental rights and freedoms » will be crucial for the outcome of balancing the legitimate interests with fundamental rights and freedoms. The outcome of the balancing test is determined by the weight given to the elements that are balanced against each other. It can be said, however, that the same provision may have a different meaning under US law and under European law (*cf. infra*, section 3). When personal data is processed on this latest legitimacy ground, individuals are granted a right to object to the data processing[12].

Data subjects have a right to access personal data pertaining to them and be informed on their personal data being processed[13]. If the controller anticipates personal data being processed for direct marketing purposes, the data subject should be offered a right to object against such data use. Other requirements concern the confidentiality, security and notification of processing[14].

The regulatory solution opted for by the drafters of the Directive was to lay down general principles that would be materialized by

11. Article 7 of the Directive.
12. The data subject must have compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer rely on that data. See article 14 (a) of the Directive.
13. See articles 10, 11, and 12 of the Directive.
14. See articles 16, 17, and 18 of the Directive.

national Data Protection Authorities (« DPAs »). DPAs have preventive and repressive tasks. Preventive tasks include offering information to individuals and companies on the interpretation and application of legal provisions, advising government bodies and legislators in domains that involve data processing, etc. DPAs also have investigative powers, and can in some Member States issue administrative penalties.

2.2. The Trans-border Data Flows Regime and the Necessity for a Comparative Law Methodology

Personal data has an intangible and ephemeral nature. The protection offered by European law would be of little effect if personal data were transferred to countries that have limited data protection. The export of personal data outside the EC is therefore subject to specific rules. These rules also apply to personal data regarding non-EU citizens that is transferred from an EU Member State.

The Directive incorporates a general principle as regards trans-border data-flows in Article 25(1) : « The Member States shall provide that the transfer to a third country of personal data which are undergoing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. »

This provision prohibits sending personal data outside the EU unless the country of destination ensures an « adequate level of protection[15] ». The *ratio legis* of this provision is to make it impossible to by-pass the Directive by exporting personal data to third countries for purposes of processing. The European legislator took the position that an export requirement is essential to guarantee the efficacy of the European data protection regime, especially in a context where personal data can easily be transferred abroad, such as in the context of the Internet or multinational companies' networks[16].

15. Or unless other facts are given : (1) « derogations » under Article 26.1, (2) « adequacy findings » under Article 25.6, (3) « adequate safeguards » taken by the data controller, specially appropriate contractual clauses, under Article 26.2, or (4) « standard contractual clauses » adopted by the Commission under Article 26.4.
16. For an analysis, see : Yves 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 (30 September 30 –

The adequacy concept determines the extent to which personal data can effectively be exported to third countries. The notion of « adequacy » contrasts with the notion of « equivalence ». Equivalent protection means that the legislator requires protection of a level which is identical to the Directive. The level of protection between EU Member States is theoretically deemed to be equivalent. However, Member States have a certain « margin of manœuvre » to decide on the means of reaching the aims set forth by the Directive.

As regards personal data exports to third countries, the Directive requires an « acceptable » level of protection, regardless of the means of protection. As Pearce and Platten put it : « [...] the adequacy principle is not intended to compel third countries to apply regulations that are identical in formal or substantive terms to the EU model – data protection may be achieved in different ways[17]. »

The Directive gives certain guidelines as regards the elements to take into account. Article 25(2) provides that « 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[18]. »

This provision states a flexible norm to assess adequacy. The final level of protection is more relevant than the means of protection used. Adequacy does not require data to be protected by state laws. Different kinds of self-regulatory techniques, such as codes of conduct, contractual arrangements, sectoral arrangements with government bodies, etc., can constitute sufficient means of protection.

October 1, 2002, Brussels). María Verónica PEREZ ASINARI, *« Is There Any Room for Privacy and Data Protection within the WTO Rules ? »*, to be published in The Electronic Communication Law Review, Kluwer, The Netherlands.

17. Graham PEARCE and Nicholas PLATTEN, *« Orchestrating Transatlantic Approaches to Personal Data Protection : A European Perspective »*, *Fordham International Law Journal*, Vol. 22:2024, p. 2028.

18. Article 26.2 of the Directive.

This approach is in line with the description made by Zweigert and Kötz as regards Comparative law methodology[19] : « [...] only the principle of functionality can let us see a solution as a whole. In particular one must resist the temptation of comparing only the statutory rules or doctrinal principles to which the various systems themselves admit [...] »[20]. Indeed, « adequacy » involves a case-by-case, pragmatic, and functional analysis[21]. This may require an adequacy assessment at the state law level, as well as at the level of a region or a private entity (for instance a company)[22]. A functional approach requires that the concrete risks of a data transfer are taken as a point of departure when assessing the legal regime of the country where the personal data is imported.

The functional approach means that one should assess the effect of the rules : the fact that a country (or a company) adheres to the principles of the Directive does not automatically mean that one should conclude that personal data is adequately protected. It may well be that the same principles, embedded in a different legal culture, have a different meaning ; or that the enforcement of the principles is limited.

Apart from the wording of Article 25(2) of the Directive, the law does not provide for any other specific methodology on how this comparative exercise must be done. We know that third countries have latitude as to the means of protection, but it remains unclear what the required substantial level of protection needs to be.

19. Konrad ZWEIGERT and Hein KÖTZ, *Introduction to Comparative Law*, Oxford, Clarendon Press, 1992.

20. ZWEIGERT and KÖTZ, *op. cit.*, p. 42.

21. Yves POULLET, Bénédicte HAVELANGE, Axel LEFEBVRE, Marie-Hélène BOULANGER, Herbert BURKERT, Cécile De TERWANGNE, *« Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des 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. This study is also available on the CRID's website : http://www.droit.fundp.ac.be/crid/privacy/default.htm (last visited 10/08/02).

22. For instance, if a company has developed and subscribed to a code of conduct, this could in theory be a sufficient ground to receive personal data from the EU. However, the interaction between state law and private initiatives is essential to assess the overall adequacy, since state law may be determinative to enforce the latter.

The Article 29 Working Party[23] elaborated criteria to determine the level of adequacy of a third country in a Working Document of July 1998[24]. The Article 29 Working Party takes the view that adequate protection comprises two basic elements : (1) the content of the rules applicable, and (2) the means for ensuring their effective application. The content principles, which are inspired from the Directive, let presume that data processing has certain universal feature (that are non-sector specific and suppose that data processing creates identical risks independent of the place and means of processing). They are the following :

(I) Content Principles

« 1. The purpose limitation principle – data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purposes of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive.

2. The data quality and proportionality principle – data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

3. The transparency principle – individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the Directive[25].

23. The Article 29 Working Party was established pursuant to Article 29 of the Directive and consists of representatives of the national DPAs and a representative of the Commission. It harmonises national data protection policy gives advice to the European legislator on initiatives that deal with data protection.

24. Article 29 Working Party, Working Document n° 12, *« Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU Data Protection Directive »*. Adopted on July 24, 1998. Available at <http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm>.

25. Article 11(2) of Directive 95/46/EC provides, in the context of an indirect data collection (i.e. data collected not directly from the data subject, but obtained from a third party data controller) for purposes of historical or scientific research, for an exemption to the obligation to inform data subjects. It is, however, required that « such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States [should] provide appropriate safeguards. »

4. The security principle – technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5. The rights of access, rectification and opposition – the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the Directive.

6. Restrictions on onward transfers – further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive. »

In addition to the content principles, the Article 29 Working Party requires that the substantial guarantees are effectively applied and/or enforced.

Can it be contended that by requiring data exporters to implement these principles, the European view on data privacy is exported together with the data i.e. the idea that the government should define a minimum level of protection to guarantee the fundamental freedoms of individuals ? In fact, the Article 29 Working Party requires that the data protection principles be present in third countries' legal systems, be it by hard law or soft law instruments, and that these principles are effectively enforced.

Can it be disputed that the Article 29 Working Party takes account of Zweigert & Kötz's methodology ? Does it pay sufficient attention to the characteristics of a specific legal system, and does it in reality subscribe to Zweigert & Kötz's functional approach ?

The answers to these questions seems to depend on the level of abstraction adhered to when considering the purpose of the data protection regulation. At the highest level of abstraction, the goal of data protection legislation is to preserve the privacy and freedoms of citizens. Pursuant to the functional approach, it is theoretically possible to have adequate protection even if the principles required by the Article 29 Working Party are not explicitly written in the law. Data subjects may be protected via other legal or extra-legal mechanisms. The law, case-law or self-regulatory measures theoretically need not *per se* contain the above mentioned data protection principles, if the individual freedoms are taken care of through other legal methods. Measuring « adequacy » at the highest level of abstraction may, for specific sectors, theoretically lead to the conclusion that a country offers adequate protection even in the absence of data protection laws. For instance, harmful data uses may be anticipated through rigid social security and anti-discrimination regulations. However, it may equally lead to the conclusion that adequate protection can never be present, because privacy and fundamental societal values are conceptualised differently in different nations.

Assessing adequate protection at this high level of abstraction may not be practical, however, because data privacy is very contextual. Data protection principles have a more procedural character and constitute practical parameters for an intercultural comparison. Obviously, these principles may have a different meaning in other legal and cultural contexts, though this does not exclude a comparison. Although the right to privacy influences the right to data protection, the latter is different from the former. Further, the risks involved in personal data processing are to a great extent universal, and require the same principles. We therefore consider that the principles must be, explicitly or implicitly, reflected in the law to qualify for an adequacy finding. This does not necessarily require the presence of a data protection law. The same ideas could be reflected through tort law or other legal or extra-legal mechanisms.

In practice, we see that the regulation of data processing in the Western world results in principles that look alike. For instance, the principles that were elaborated in 1995 by the Information Infrastructure Task Force[26] are, albeit offering lower protection, similar

26. See http://www.eff.org/Privacy/GII_NII/iitf_principles.draft, (last visited 21/09/02). File posted at the request of the Information Infrastructure Task Force's Privacy Working Group, chaired by Robert Veeder, Office of Management and Budget.

to the OECD data protection principles and the principles of the EU Data Protection Directive.

A famous decision of adequacy exists in the US, namely the « Safe Harbour Agreement »[27]. US controllers adhering to the principles can receive and process personal data from the EU. US controllers therefore need to implement the basic principles set out in the agreement, including requirements on notice, choice, security, onward transfer, data integrity, access, and enforcement. It presents many particularities, mainly the fact that it does not cover the whole US legal system of privacy, and that it installs a different regime for data streams coming from the EU. The safe harbour principles are supplemented by « FAQs » (*Frequently Asked Questions*), published by the Department of Commerce and providing guidelines for the implementation of these principles. Adherence to the principles by US companies is voluntary. When subscribing to the principles, companies must reveal their confidentiality rules and fall within the competence of the Federal Trade Commission.

III. The EU and US Legal Framework Compared

We have already mentioned that both the European and US legal systems have a divergent approach to privacy and data protection. To understand the differences between the EU and the US, an interdisciplinary analysis is necessary, covering historical, philosophical, sociological, anthropological, political, economic, and other aspects. A functional comparison requires that the rules be contextualised to understand their exact meaning. This part demonstrates that although there are data privacy laws in the US, such laws are conceived differently from that which exists in Europe. While data privacy is considered a human or fundamental right in Europe, it is considered a consumer interest in the US. We believe that the dichotomy between the US and the European approach creates and maintains strong divergences between both sides of the Atlantic.

27. 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.

3.1. The Right to Privacy and Data Protection : a Human Right or a Consumer Interest ?

The question whether data privacy constitutes a human right, or should only have a lower status and be seen as a consumer or individual interest lies at the core of EU-US dialogue[28]. The qualification of data privacy as a human or fundamental right has an important impact on the status of the rules regulating data privacy. They would then take on a compelling character and it would be excluded to go below the level of protection provided for in the law. In addition, a human or fundamental right's status has, from a legal and/or political point of view[29], important weight to require protection regardless the geographical place where the data is processed (human rights are considered to be « universel »).

In this section we will analyze data protection in Europe

A. European framework

In Europe, privacy as well as the right to personal data protection are considered to have human rights status. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms defines it in the following way : « (1) Everyone has the right to respect for his private and family life, his home and his correspondence » [30]. This article has been extensively interpreted by the European Court of Human Rights, giving a wide dimension to the concept of private life[31]. Article 8 ECHR is self-executing, and takes

28. See for instance, Andrew CHARLESWORTH, *« Data Privacy in Cyberspace : not National v. International but Commercial v. Individual »*, Law and the Internet : A Framework for Electronic Commerce (2nd. ed.) eds. Edwards L. and Waelde (Oxford : Hart Publishing, 2000), pp. 79-122 ; Serge GUTWIRTH, *Privacy and the Information Age*, (Lanham, Md. : Rowman and Littlefield Publishers, 2001).

29. Whether this argument has legal or only political status depends on the legal theory one is adhering to. The argument would be legal in a Ius Naturalis discourse, but only political in a positivist theory.

30. Convention for the Protection of Human Rights and Fundamental Freedoms ETS n° : 005, Rome 4/11/50. Available at <http ://conventions. coe. int/ treaty/en/WhatYouWant.asp?NT=005>.

31. European Court of Human Rights, Case *Amann v. Switzerland* (Application n. 27798/95), Strasbourg, 16 February 2000 ; Case *Rotaru v. Romania* (Application n. 28341/95), Strasbourg, 4 May 2000 ; Case *P.G. and J.H. v. The United Kingdom*(Application n. 44787/98), Strasbourg, 25 September 2001, etc. See also Paul DE HERT, « Art. 8 EVRM en het Belgisch Recht, de

precedence over conflicting national legislation, including national constitutions[32]. Citizens can rely and invoke these provisions before a judge against public authorities. Some European countries, such as Belgium and the Netherlands, adhere to the theory of « Drittwirkung », according to which these articles have a horizontal effect, meaning that they also have an impact on relations between citizens.

Following the doctrine of « positive obligations », signatories to the Convention have the positive obligation to protect the private lives of their citizens. These obligations do not merely extend to relations between public authorities and citizens, but also apply to *intra-citizen* relations. Accordingly, the State is obliged to intervene if one individual threatens the privacy of another individual. These provisions do not explicitly refer to the protection of personal data or informational privacy. However, informational privacy is considered to fall under these provisions. This has been confirmed by the European Court of Human Right on many occasions[33].

The Council of Europe further passed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data n°108, which deals with the protection of personal data[34]. This Convention sets forth specific requirements as regards the processing of personal data and gives substantial meaning to Article 8 ECHR in the context of informational privacy[35]. It contains the general principles and rules that, together with the OECD guidelines on Data Protection, have served as a source of interpretation of Directive 95/46/EC (the first international *mandatory* document)[36].

Bescherming van Privacy », *Gezin, Woonst en Communicatie*, Mys & Breesch, Ghent, 1998.

32. Serge GUTWIRTH, *op. cit.*, p. 35.

33. For instance Eur. Court HR, *M.S. v. Sweden*, Judgment of August 27, 1997, Reports of Judgments and Decisions 1997-IV ; Eur. Court HR, *Rotaru v. Romania*, Judgment of May 4, 2000, application n° 28341/95.

34. Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS n° 108, Strasbourg 28-01-1981. Available at <http ://conventions.coe.int/treaty/ en/Treaties/Html/ 108.htm>.

35. The purpose of Convention n° 108, as stated by Article 1, « is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection'). »

36. Many recommendations issued by the Council of Ministers offer interpretations of the Convention's Principles in specific areas such as the medical sector,

Pursuant to Article F of the Treaty of the European Union, the EU is required to respect the European Human Rights Convention[37]. The first two paragraphs are of particular interest to data protection and privacy :

> 1. « The Union shall respect the national identities of its Member States, whose systems of government are founded on the principles of democracy.
>
> 2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law. »

The consequence of this important provision is that although Directive 95/46/EC is primarily an Internal Market instrument, EU data protection policy is highly influenced by human rights concerns. Therefore, its provisions should be mirrored in the light and spirit of the European Human Rights Convention. EU Member States are responsible *vis-à-vis* the Council of Europe, for the respect to the Conventions of the aforementioned. Indeed, Article 1 of the Directive confirms that « Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data »[38].

Recently, he European Union adopted a Charter of Fundamental Rights, including not only the right to privacy but also the protection of personal data[39].

direct marketing, genetic data, etc. These recommendations are not binding, but serve as important guidelines to develop and interpret legislation.

37. The relation between the Strasbourg and the Luxembourg Courts in what concerns their competences on human rights remains controversial. It remains debated to what extent a decision of the Luxembourg Court could be revised by the Strasbourg Court.

38. Explicit reference to Convention n° 108 can be found in Recital 11 of the Directive. Economic impact is not analysed in the opinions of the Article 29 Working Party, because these opinions have no binding status.

39. The full text of the Charter of Fundamental Rights of the European Union, *OJ* C 364/1, 18-12-2000:<http://europa.eu.int/comm/justice_home/unit/charte/pdf/texteen.pdf>. See also : Working Party on the Protection of individuals with regard to the Processing of Personal Data (hereinafter « Article 29 WP ») *« Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights »*, Adopted on 7 September 1999, available at http://www.europa.eu.int/comm/internalmarket/en/dataprot/wpdocs/wp26en.htm.

Article 8 of the Charter provides :

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

Regardless of the legal nature of the Charter, it constitues further evidence of the political position of the EU in this domain[40] [41]. The Charter is important for at least two reasons : first, it confirms the political will to recognize the right to data protection as an autonomous fundamental right in the Community legal order. Second it is absolute in its wording and highlightts the role of an independent authoritory to effectively enforce data protection principles.

The constitutional traditions of the Member States are another important element that should be contemplated when assessing European tradition, since many Member States' constitutions include privacy and/or data protection explicitly[42]. Concretely, the concept of « informational self-determination » endorsed by the German Federal High Court (*Bundesverfassungsgericht*) has considerably influenced the Directive's architecture, as well as the importance of the right of informational privacy[43]. This concept holds that an individual should have a right to control « the image of his personality » that is presented through the processing of his personal data. Individual control implies that all processing modalities are transparent and known, and agreed and verifiable by the data subject. The doctrine is based on fundamental

40. *Commission Communication on the legal nature of the Charter of fundamental Rights of the European Union* 11/10/2000, COM (2000) 644 Final. Available at:http://europa.eu.int/comm/justicehome/unit/charte/pdf/com2000644en.pdf>.

41. *« Finalement, la Charte des droits fondamentaux, telle qu'adoptée lors du Sommet de Nice, n'a pas d'effet contraignant ; il faut néanmoins s'attendre à ce qu'elle exerce une certaine influence sur la pratique juridique. »* Hans C. KRÜGER and Jörg POLAKIEWICZ, « Propositions pour la création d'un système cohérent de protection des droits de l'homme en Europe » *Revue Universelle des Droits de l'Homme*, Vol 13 n° 1-4. 2001, pp. 1-14.

42. Portuguese Constitution, Article 35 ; Spanish Constitution, Article 18 ; Belgian Constitution, Article 12 ; Dutch Constitution, Article 10 ; etc.

43. BverfG., EUGRZ, 1983, p. 588.

respect for the individual's autonomy and person. The theory of informational self-determination is reflected in the Directive's consent principle : consent is the most important legitimacy ground for the processing of personal data. This perspective explains why a mere tort law approach, which offers means of redress *post factum*, is deemed insufficient in the EU : respect for the individual requires that the individual's choice as regards the processing of personal data pertaining to him/her is respected, regardless the presence of harm.

The fact that privacy is deemed a human right implies that protection of this good is a case of public order. Although a certain preventive effect may result from tort law enforcement (especially if punitive damages are used), the several arguments plead against protection via tort law actions : (1) the burden of proof is inversed to individuals, (2) it risks that « harm » is defined and indirectly defines and restricts « privacy », (3) harmful data uses may be deemed non-harmful because legislators or judges confuse these data uses with other legal/societal norms, and (4) harm is a subjective and contextual notion.

B. Data Protection in the US

Contrary to Europe, the US does not consider data privacy as a human right, nor does it have a general data protection framework comparable to the Framework Directive in Europe. The American Convention on Human Rights (« Pact of San José, Costa Rica »)[44] mentions the protection of private life in Article 11 as follows :

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.

44. 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 was adopted in the context of the Organization of American States (OAS), and it has been ratified by all the Latin American signatories, see <http ://www.oas.org/juridico/ spanish/firmas/b-32.html>.

Although the US has signed this instrument, it has not ratified it. Consequently, the Convention has no legal status in the United States[45].

US data protection law is characterized by complexity rather than absence of regulations : « Rights and responsibilities for fair information practice will emerge from any of several categories of law at either the federal or state level. Constitutional as well as statutory law exists at both levels of governance. In addition, at the state level, court interpreted common law rights may exist. Citizens rights may be protected separately through federal or state law and collectively through combinations of federal and state law »[46].

In the US, privacy has been more severely protected in vertical relations (public law) than in horizontal relations (private law).[47] Specifically, the US Constitution « prevent[s] the government from encroaching upon an individual's rights ; [it does] not require the government to protect those rights against third parties[48] ». The grants Constitution does not contain an explicit right to privacy, and considers great importance to freedom of expression, set forth by the first Amendment. The federal Supreme Court reads, however, a right to privacy in the US Constitution, protecting individuals against government intrusions. Further, the state constitutions of Arizona, California and Illinois expressly protect privacy, though only in vertical relations.

Schwartz and Reidenberg distinguish four areas of constitutional data protection law : 1) associational privacy ; 2) voting rights ; 3) the Fourth Amendment; and 4) informational privacy[49].

45. See : General Information of the Treaty : http://www.oas.org/juridico/ spanish/ firmas/b-32.html.
46. Joel REIDENBERG and Paul SCHWARTZ, *« Study of American Personal Data Protection Law »* under the direction of Prof. Dr. Spiros SIMITIS, Research Centre for Data Protection, Frankfurt am Main, Germany, Johann Wolfgang Goethe-Universität, 1994.
47. The tradition of Lockean liberalism in the United States supported checks on public power and only narrow restraints on private power. See REIDENBERG and SCHWARTZ, *Study of American Personal Data Protection Law*, *op. cit.*, p. 3.
48. Andrew CHARLESWORTH, *op.cit.*, p. 92.
49. Paul M. SCHWARTZ and Joel R. REIDENBERG, *Data Privacy Law. A Study of United States Data Protection,* Viriginia, Michie Law Publishers, 1996.

The *first area*, associational privacy, has been divided into two branches by the Supreme Court : *« First, there is a 'freedom of intimate association', which has its basis in the Bill of Rights. Second, there is a 'freedom of expressive association', which has its basis in the First Amendment*[50] ».The text of the latter says : *« Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof ; or abridging the freedom of speech or of the press ; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances »*. The Supreme Court has thus prevented the state from collecting information that would unconstitutionally compel a disclosure of group affiliation[51].

The second area, voting rights, is covered by the Equal Protection Clause, the Due Process Clause, and the First Amendment. *« The health of a democratic system requires limitations not only on the use of information regarding group political activity, but also on the use of information regarding the exercise of the electoral franchise. This scrutiny is necessary because certain kinds of information use can impinge on the right to vote and thereby directly interfere with the individual's participation in political self-governance. In the United States, voting records are maintained at the state level. A state practice of* collecting or applying personal data *that interferes with the right to vote should be subject to searching judicial scrutiny*[52] *»*.

The third area is within the scope of the 4th Amendment, which states as follows : *« The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized »*.

The fourth area, informational privacy, was identified by the Supreme Court in its decision *Whalen v. Roe* (1977). *« This case concerned a New York law that created a centralized state computer file of the names and addresses of all persons who obtained certain drugs*

50. SCHWARTZ and REIDENBERG, *Data Privacy Law. A Study of United States Data Protection, op. cit.*, p. 44.

51. *Ibid.* The leading case remains *National Association for the Advancement of Colored People (NAACP) v. Alabama* 357 U.S. 449 (1958).

52. SCHWARTZ and REIDENBERG, *Data Privacy Law. A Study of United States Data Protection, op. cit.*, p. 54.

pursuant to a doctor's prescription. While upholding the state's exercise of power, the Supreme Court found this governmental gathering of information to affect two interests. One was an 'individual interest in avoiding disclosure of personal matters' ; the other, 'the interest in independence in making certain kinds of important decisions.' These two interests rest on the Bill of Rights' protection of substantive due process in the Fifth and Fourteenth Amendments »[53].

As we can see, the US Constitution does not explicitly protect the right to data privacy, yet different ways of protection have been created through the interpretation of the Supreme Court. The Constitution does not protect against private persons, but only against government actions[54].

These intrinsic differences are at heart of the EU-US dialogue or « dispute » on privacy and data protection. The fact that privacy is considered a human right in Europe explains why the regulation on trans-border data flows are designed in such a way to assure that European data will receive sufficient protection when it crosses the geographic boundaries of Europe. The absence of a general regulation in the US, as the one given by the Directive, has other consequences.

Firstly, the fact that data privacy is deemed to be a human right affects the way in which an adequate regime of protection is perceived. Clearly, the perspective between the European and US view on data protection is different : in Europe, data privacy is considered more from the perspective of the data subject, while in the US it is considered in its economic context. In general, US privacy law adheres to a different anthropological conceptualisation. This means that, for instance, in the area of e-commerce the data subject is only considered as a « consumer ». In Europe, privacy or personal data, is considered to

53. SCHWARTZ and REIDENBERG, *Data Privacy Law. A Study of United States Data Protection, op. cit.*, p. 76.

54. *« Two general characteristics of American constitutional law have played a role in shaping the extent to which higher law in the United States has influenced data protection. The first aspect concerns the Constitution's placement of limitations generally on the government alone rather than on private organizations. Constitutional rights usually are not applicable unless 'state action' has taken place. The second pertinent characteristic of constitutional rights in the United States is that even when applicable, these interests generally do not require the state to take positive action. They prevent certain kinds of governmental action, but place no affirmative duties on the state. »* SCHWARTZ and REIDENBERG, *Data Privacy Law. A Study of United States Data Protection, op. cit.*, p. 32.

be outside trade. The fact that individuals consent to the processing of their personal data does not imply that they contract away their privacy. The European Data Protection Directive is *d'ordre public*, and data controllers need to implement its requirements, regardless of whether obtain the individual's consent or not.

Secondly, the presence or absence of actual harm resulting from data processing is not a relevant criterion in Europe to permit or prohibit certain data processing activities. Privacy is deemed protect-worthy, even if the harm to data subjects resulting from data processing is relatively limited or difficult to measure in order to quantify damages. The impact of this provision is important in practice : when assessing the legitimacy, proportionality, security, etc., of data processing, the interests of the data controller have less weight than the fundamental right to privacy of the individual.

We believe that the perception of privacy in terms of a human right also has an impact, among other aspects, on : (1) torts ; (2) self-regulatory approach in the field of e-commerce ; and (3) interpretation of data protection principles.

3.2. Data Protection via Tort Law Actions

In Europe, a violation of the data protection principle set forth by the Data Protection Directive, and/or Article 8 ECHR is actionable under tort law. The Directive sets forth a specific provision on liability :

> « 1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
>
> 2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage[55] ».

According to Grimalt Servera the legal regime followed by the Directive is a no-fault liability but limited to the fact that an effective violation of one of the Directive's regulation would have taken place[56].

55. Article 23 of the Directive.

56. Pedro GRIMALT SERVERA, *La responsabilidad civil en el tratamiento automatizado de datos personales*, Granada, Editorial Comares, 1999. The author follows the former Spanish law (LORTAD), however, the regulation on this point uses the same principle.

The Directive would inverse the burden of proof requiring the controller to demonstrate he did not violate the Directive's provisions or that a third party bears liability. However, it remains debated whether this provision creates no-fault liability regime, or merely constitutes a restatement of the fault liability regime common in all EU Member States.

In the US, tort law has greater importance than in Europe as regards the right to data protection. Where enforcement of data protection rights in a tort law paradigm is rather a consequence than a source in Europe, US privacy law has been conceptualised through the law of torts in horizontal relations (i.e. between private parties). Typical to tort law protection is that it offers a remedy *post delictum*, and that the burden of proof lies with the individual. Where in Europe data subjects can theoretically introduce a tort law action in case of any informational privacy infringement that results in physical or moral damage, US tort law actions are limited. *The Restatement (Second) of Torts*[57] has classified privacy torts in four categories : (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light privacy, and (4) misappropriation of name or likeness for commercial purposes[58]. In these four cases, for a tort to be present, the privacy invasion must be highly offensive to a reasonable person. Since privacy is contextual and valued differently, even amongst « reasonable persons », this criterion may create uncertainty. Apparently, this requirement lowers the threshold of protection.

According to the Restatement of Torts the offence of intrusion upon seclusion is defined as « one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person ». Pursuant to the Restatement's comments, a privacy invasion includes a physical invasion, such as entering a person's home, an invasion accomplished through the offender's senses, such as eavesdropping, wiretapping, or peering in someone's windows, or by some investigation or examination of a person's

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

58. Erika S. KOSTER, « *Zero Privacy : Personal Data on the Internet* ». Available at <http ://www.oppenheimer.com/intprop/news/zeroprivacy.shtml> (last visited 10/08/02).

private affairs, such as reading someone's mail or accessing their bank account information.

In Europe, all personal data is protected, regardless of the fact that the data is confidential or not; in the US, only data that has a confidential or secret character is protected by this first tort. In *Dwyer v. American Express Co.*, it was held that it was not a tortuous appropriation of personal information to include credit card holder's names in categorized marketing mailing lists, because credit card holders « voluntary and necessarily disclosed information by using the card »[59]. In *Biddle v. Warren General Hosp.*, the court held that it is a breach of patient confidentiality rather than an invasion of privacy when a doctor tortuously provides non-public information to a third party who does not have the privilege to receive such information[60].

The second tort requires a disclosure of private facts. Here too the disclosure must be such that the private fact is « substantially certain to become one of public knowledge[61] ». Further, « where the publicity is so offensive as to constitute a morbid and sensational prying into private lives for its own sake it serves no legitimate public interest and is not deserving of protection[62] ». The Restatement of Torts stipulates examples of categories of data which public disclosure is exempted from liability, and those that are not : exempted are date of birth, marital status, military record, professional or occupational license and criminal proceedings. Income tax returns, information on sexual relations and unpleasant or disgraceful or humiliating illnesses, are subject to potential liability upon disclosure. It is to be noticed that the effective harm or specific context is not considered for the first category of information.

The third tort requires that « one who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if the

59. *Dwyver v. American Express Co.*, 652 N.E. 2d 1351 (1995). This decision dates from the dawn of the Internet-era, and it is not sure that the same would be decided today.

60. *Biddle v. Warren General Hosp.*, 86 Ohio St. 3d 395 (1999).

61. *Tureen v. Equifax*, Inc. 571 F. 2d 411 (8th Cir. 1978), dissemination of plaintiff's life and health underwriting history report to health insurer by consumer credit reporting firm held insufficient publication.

62. *Diaz v. Oakland Tribune*, Ind., 188 Cal. Rptr. 762, 767 (Cal.Ct. App. 1983), mentioned in Erika S. KOSTER, *op. cit.*, p. 6.

false light in which the other was placed would be highly offensive to a reasonable person, and if the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed »[63].

The fourth privacy tort doctrine applies to the use of an individual's name or likeness without consent. However, the unconsented re-utilization of data for purposes other than those for which the personal data was collected does not *per se* constitute a tort, especially, if personal data is deemed not to have an economic value. This being the case, an individual cannot successfully prevent his personal data from being disseminated by arguing a taking has occurred or that he is permanently deprived of the commercial value of that data. This holding makes a misappropriation challenge virtually impossible. Data subjects would most likely not be granted relief on this tort, unless they could prove that their personal data had been utilized to obtain commercial benefit at some sort of scale[64].

Annex IV to the Safe Harbor Agreement contains an answer to the European Commission's request for clarification of US law with respect to claims for damages for breaches of privacy. When explaining the common law torts it says : « 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' »[65].

This paragraph demonstrates the limitations of common law torts enforcement of data protection rights. For instance, if the disclosure is

63. Restatement (Second) of Torts, § 652E (1977).

64. See Erika S. KOSTER, *op. cit.*, : « The misappropriation doctrine could theoretically provide a basis for liability for the sale of non-public personal information collected by web sites and, indeed, it seems to be the most likely avenue to challenge this activity. However, attempts to challenge distributors of mailing lists have not been successful. A key influence in these decisions, however, seems to have been the assumption that a particular individual's data had no value and thus the individual was not deprived of anything when the information was aggregated and rented to interested parties. »

65. Italics added.

not « highly offensive » to a « reasonable person » the damage would not be enforceable. Those subjective expressions also pose questions regarding their extent and criteria to determine what kind of disclosure can be qualified in this way.

The fact that in European law systems torts are not limited to specific cases[66] may explain why the safe harbour principles are not enforced through common law torts actions, and why it was necessary to find other adequate remedies. The solution was to use the fair commercial practice doctrine to enforce the principles. Pursuant to this doctrine, failure to comply with the principles after a public representation to implement them is actionable under Section 5 of the Federal Trade Commission Act[67] prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.

In addition to the limited scope of tort law in the US, these torts are not explicitly meant to deal with data protection issues, but rather with privacy infringements. Tort law risks reducing privacy to a « subjective right » (French « droit subjectif ») because harm needs to be defined to give practical meaning to the law. Typical of « subjective rights » is that the object of the rights need to be defined (e.g. a definition of property is required to claim that any interference/damage to your property constitutes a violation of your subjective right to your property). The harm-based approach in fact defines « privacy », be it negatively. The Data Protection Directive, however, establishes principles that apply regardless of the harm that individuals suffer ; it is based on a general idea of respect for the individual's human dignity and self-determination.

66. Consideration also has to be given to « hundreds » of privacy laws both at federal and state level, the violation of which could give rise to civil liability. Many of these laws allow individuals to sue for damages when violations occur : e.g. Fair Credit Reporting Act (1970), Fair Credit Billing Act (1974), Equal Credit Opportunity Act (1974), Right to Finantial Privacy Act (1978), Video Privacy Act (1988), Electronic Communications Privacy Act (1986), Cable Communications Policy Act (1984), Telephone Consumer Protection Act(1991), Gramm-Leach-Bliley Act (1998), Children's Online Privacy Protection Act (1998).

67. Annex III to the Safe Harbor Agreement describes the FTC competence over unfair or deceptive practices.

3.3. Self-Regulatory Approach in the Field of E-Commerce Privacy

The functional comparative law approach requires analysis of other forms of regulation, such as self-regulatory techniques and contracts. To assess adequacy under the transborder data flow requirements, private or non-state regulation must be considered. We believe that data privacy being considered a fundamental right has not only an impact on the content of the law, but also on the regulatory means to protect privacy. For instance, despite the Directive's Article 27, self-regulation is less popular in the EU because the level of protection set forth by the Directive and Convention N°108 constitutes a minimum[68]. Indeed, within the field of data privacy, « self-regulation » tends more to « co-regulation », meaning that private initiatives are assessed and approved by national/European authorities.

Unlike European society, the US adheres to a libertarian conception of freedom, according to which every action that is not prohibited is allowed[69]. In this context, data processing is, in principle, not subject to any regulations, unless it would be harmful or be subject to these specific laws. Self-regulatory initiatives constitute a procedural technique of privacy protection, without guaranteeing a minimum level of data protection. Fairness requires that processing of data be done in accordance with announced data handling practices. However, fairness is rather construed as a procedural requirement than a substantial requirement, and does not require a minimum level of protection. Unlike a European citizen, US citizens can, except in cases where sector specific laws apply, consent that data pertaining to them is unconditionally used for any other purpose.

The White House issued a document during the Clinton Administration, defining its political orientation in the field of e-commerce : « A Framework for Global Electronic Commerce »[70]. This

68. See Article 27(3) of the Directive : « Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. [...]. »

69. In Europe, data processing is permitted only if one has a legitimate basis to conduct a certain processing activity.

70. *« A Framework for Global Electronic Commerce »*, The White House, July 1, 1997. Available at http ://www.ecommerce.gov/framewrk.htm, last visited 23/08/01.

document was drafted in liberal terms and set forth that (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. Although it confirmed the liberal hallmark of American legal thinking, it also reflected the idea of consumer confidence to keep e-commerce thriving.

The document stressed the importance of balancing privacy with the benefits associated with the free flow of information. It acknowledged that privacy was important, and set forth that individuals should be aware of the collection and processing of their personal information, and that they should have some meaningful way to limit use and re-use of that information. It proclaimed a policy that was based on self-regulatory initiatives and technological means to protect privacy, and limited the intervention of the state to a minimum[71].

As a consequence of the political orientation, and encouraged by the Federal Trade Commission, many self-regulatory initiatives have flourished : codes of conduct, privacy policies, networks (see NAI[72]and OPA[73]), and labelling systems, such as : TRUSTe[74],

71. « The Administration supports private sector efforts now underway to implement meaningful consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the existence of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution. » « The Administration also anticipates that technology will offer solutions to many privacy concerns in the online environment, including the appropriate use of anonymity. If privacy concerns are not addressed by industry through self-regulatory and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online. » « To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled. » See : « A Framework... », *op. cit.*,

72. « The NAI (Network Advertising Initiative) is a cooperative group of network advertisers. It developed a set of privacy principles, in conjunction with the Federal Trade Commission. The NAI's foremost commitment is to provide consumers with clear explanations of Internet advertising practices and how they affect you and the Internet itself. » See : http://www.networkadvertising.org/, last visited 12/10/02.

BBBOnline[75], etc. These labelling services consist mainly in providing a seal or trust-mark visible on the screen to the sites that adhere to established privacy principles, which is a guarantee for the observance of the principles and enforcement mechanisms.

In the US, it is up to the consumer to search for the better protection available in the market.

The EU gives some room to self-regulation. Indeed, the Directive states that :

> « 1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors »[76].

However, where self-regulation is classically used as a pretext to avoid any additional state intervention or strict regulation, EU codes of conduct regarding data protection cannot lower the level of protection

73. « Upon joining the Online Privacy Alliance, each member organization agrees that its policies for protecting individually identifiable information in an online or electronic commerce environment will address at least [the following] elements, with customization and enhancement as appropriate to its own business or industry sector. » See : http://www.privacyalliance.Orgresources/ppguidelines.shtml, last visited 12/10/02.

74. « A cornerstone of our program is the TRUSTe 'trustmark', an online branded seal displayed by member Web sites. The trustmark is awarded only to sites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures. Privacy principles embody fair information practices approved by the U.S. Department of Commerce, Federal Trade Commission, and prominent industry-represented organizations and associations. » See : http://www.truste.org, last visited 12/10/02.

75. « For consumers shopping on the Internet, privacy is a major concern. Almost three-quarters of Internet users are concerned about having control over the release of their private information when shopping online. (Source : U.S. Census Data). Your customers want assurances that you protect their information before they decide to make a purchase. The first step is to tell online shoppers that you value the privacy of their personal information through an easy-to-understand and easy-to-find privacy policy. Better yet, let the Better Business Bureau tell them! The BBB*OnLine* Privacy program was developed specifically to help business web sites address this key concern of online shoppers.» See : http://www. bbbonline.com, last visited 12/10/02.

76. Article 27.1 of the Directive.

set forth by the Directive. Nonetheless they may better implement the Directive's requirements in specific cases. For instance, a code of conduct on direct marketing may be more appropriate and effective to regulate DM activities than state law regulations. They can extend the protection, but obviously, not reduce it.

As a consequence, even if the market provides for a high level of protection, active intervention of the data subject will be necessary for the protection to be effective. From the European perspective this generates a burden for the individual, not only by having to read the level of protection guaranteed by different actors in the market, but also by having to understand the legal jargon.

IV. Concluding Remarks

The « new physics » that has come in the tow of the Internet creates a new reality whereby distance and time are constantly bridged and differences in culture and law become apparent. However, the absence of digital boundaries does not imply the absence of geographical boundaries with their own legal systems and competent authorities. In this contribution, we first had a glance at the EU and US legal framework for privacy and data protection, exercising a comparative methodology. At this stage, we can make four concluding remarks :

1. International data protection requires a sound comparative law methodology to understand how different legal systems address privacy risks derived from international communications and transactions. Such an understanding is necessary not only to appraise those risks, but to allow consensus building in the search for solutions to adequately protect personal data in open networks.
2. The notion of « adequacy » included in Directive 95/46/EC pushes for constant comparison of law, not only from a theoretical point of view, but also from a practical day-by-day business point of view. « Adequacy » requires looking deep into a third country legal system to understand what the rules concretely mean and how they are or would be applied, to analyse whether they are « adequate » for the EU legal framework, in order to make an international transfer of personal data.

3. The different conception concerning privacy and data protection in terms of human right and/or civil liberty, and consumer rights has consequences not only in the extension of the protection provided by the law, but also as regards the regulatory approach. Where self-regulation, for example in the field of e-commerce, is very limited in the EU, it is encouraged in the US. Further, codes of conduct would be integrated as an example of co-regulation in the EU, and of self-regulation in the US.
4. Questions remain whether these « new physics » will lead to a unified body of Internet law, in general, and/or privacy law, in particular. Zweigert and Kötz elaborate on and structure the practical benefits of comparative law[77]. The fourth benefit mentioned by these authors is its contribution to the systematic unification of law. Considering that privacy and data protection are domains where l'*ordre public* has a strong presence[78], unification or harmonization is difficult and slow, especially if political incentive is limited or absent. However, this possibility has to be borne in mind. An international convention or « model law » would solve many of the intricate problems (including legal uncertainty) inherent in adequacy assessments. The challenge is how cultural and legal traditions would be respected.

77. ZWEIGERT and KÖTZ, *op. cit.*, p. 15.
78. At least in the EU, Eastern European countries, Latin American countries, etc.