ELECTRONIC COMMERCE AND PRIVACY[1]

Y. POULLET
Prof. at the University of Namur
Director of the CRID

1. Internet is becoming more and more like an enormous and infinite commercial fair with innumerable services around the globe, accessible through the Web[2].

If Internet commerce is considered to be still small[3], even the more conservative ones consider that the growth of electronic business especially as regards Business-consumers far above the average growth of overall turnover[4]. The electronic commerce will not only create new activities but also deeply affect the way for conducting business.

This success is due to the fact that the WWW is built on two non sophisticated premises : the so called HTTP and HTML[5]. Firstly, the HyperText Markup Language (HTML) is a uniform format for all material of the Website and permits that all information, requests and responses conform to the same standard and might be read by each equipped computer by simple userfriendly interface. That is a unique code being used to describe a Web page content which is interpretated and displayed by a Web browser.

Secondly, the HyperText Transfert Protocol (HTTP) is defined as the protocol used between a Web browser and a Web server. The Web brower is sending HTTP request to a Webserver and is obtaining an HTTP answer including namely but not only (we will come back to that problem) the Web page in HTML code.

Thanks to these two simple but powerful premises, users may surf without limits and borders on the Web (This activitiy represents more than 80 percent of the Internet's traffic). They all use standardised protocols like

---

[1] Les recherches menées ici s'inscrivent dans le cadre des études menées par le pôle d'interuniversitaire "Société de l'information" qui regroupe la CITA, le CRID des FUNDP, le LENTIC de l'Ulg et le SMIT de la VUB (Brussels) financé par les S.S.T.C., administration de l'Etat belge.

[2] The present paper has submitted both to the Conference organized by the « Garante per la protezione dei dati » (Roma, 8-9 May 1998) ; « Internet and Privacy : which rules » and by the IFCLA, at Oslo the 18-19 June « electronic Commerce : the real Trade ».

[3] The present estimate range of annual turnover (some $ 26 billions) will grow rapidly and may approach a trillion dollars by 2003-05 (http://www.inforworld.com/cgi-bin/displaystory.pl ? 980511.ciecomm.htmkl and OECD, The economic and social Impact of Electronic Commerce : preliminary findings and research agenda – Executive Summary, Ottawa, Canada, 7-9 oct. 1998).

[4] Recent studies (http://www.newsbytes.com/pubNews/98/112154.html ?st.ne.fd.mnaw ;OECD (GD(97)219,p.7) does estimate that 10% of the worldwied retail and wholesale market will be done electronically through Internet. The number of connected computer has been estimated recently (July 98) to be about 130 millions (http://www.neca.ie/surveys/how_many_online/index.html).

[5] HTTP and HTML specifications have been defined by the World Wide Web consortium (W.3.C.) as de facto standards adopted after different in Request for Comments. It is too be underlined that the Software editors are broadly represented.

TCP/IP (Transmission Control Protocol/Internet Protocol) which enables each connected computer to dialogue with another connected computer irrespective of the receiver's operating system[6].

2. Our aim is not to describe in detail all the privacy problems deriving from the multiple E. Commerce activities. Definitively, we will not analyze to what extent the present European directives are applicable to Internet[7] but only to suggest new ideas and trails of research on three points:

- the first one underlines how new actors, new technical possibilities are creating new risks and privacy threats;
- the second one envisages the regulatory solutions: Internet does challenge our legal framework, claiming new basic principles but also suggesting certain audacious interpretations in order to cover new features;
- the third one would like to introduce new criteria to evaluate the selfregulatory solutions and privacy enhancing technologies.

I. New Actors, new technical possibilities and new privacy risks and threats

- **The actors**

3. The large number of actors – or to be more precise of functions - intervening in the electronic transactions is definitively an important factor we have to take into account. The number of persons intervening multiplies the number of processing and certain of these processing are not identified as such by the user, or to take the expression usually used in electronic commerce: the customer.

4. Indeed, beyond the actors directly involved in the commercial electronic transaction: the "customer" and the "seller" (in the broadest sense insofar as by seller one means also an administration or a web site delivering information or publicity without any intention to conclude commercial transactions), other secondary actors involved in electronic transactions have to be identified:

- the **Internet Access Providers** (IAP) will provide to the users the technical net-infrastructure to get access to the Internet[8]. Frequently they are also providing the Internet software necessary to be able to browse on the internet. For their own security, they might keep a trace of the different uses carried out by the webuser. They might be sollicited by the public authorities to maintain the storage of these data in order to facilitate criminal investigations;

[6] Practical Guide to Legal Issues of Electronic Commerce, ECLIP Study developed by I.T.M. (Univ. of Münster) to be published.
[7] On that point, see the annex developed by S. Louveaux, Privacy Issues, ECLIP Study.
[8] In order to do so, I.A.P. maintain so called « points of presence » (POP), local connections points to the Internet in order to provide local cheap access (for a comprehensive list of IAP, see http:// thelist.internet.com/).

- the "**carriers**", that is to say the telecommunications organisation which provide basic networks for data transfer[9];
- the "**Internet service providers**" (ISP) supply services for storage, transmission and presentation. They are hosting Web sites developed by Content Providers (ICP) and might intervene as regards the routing of the messages, the processing of traffic data or the billing of the different transactions;
- the **Web sites offering search engines**[10] which are becoming more and more popular due to the vast amount of information on almost every topic and the absolute need for the "customer" to easily find the correct searched information[11]. These specific web sites create two risks: the first one is the fact that they have the possibility to collect data on an individual data widespread in various places and to infer a profile of this individual; the second one is the capability for providers of these search engines to draw up a detailed profile of the interests expressed by their users.

- the **banks or financial institutions** might also be involved in the process of an electronic commerce transaction, insofar they are authorizing the payment after having checked the financial capability of their customers.

5. Before describing a third category of actors, let us underline the fact that a same actor may offer different services (e.g. telecommunications operator and internet services provider or internet access provider and internet services providers) himself or through subsidiairies. The consequence of this fact is that it will create difficulties to identify the multiple links and flows between actors belonging to a same consortium and between functions exercised by the same actor.

6. The need to create trust and confidence in the electronic commerce does suggest the intervention of a third category of actors : the certification authorities, the thrusted third party and also auditor labelling the web site following different criteria, especially in the context of this article, the « privacy » regulatory requirements enacted either by a selfregulatory instrument (code of conduct) either by a legislative decision.

The « Trust-e» label has to be pointed out in that context. This label[12] has been developed by a consortium founded by different companies like IBM, NETSCAPE, IMGIS, America Online, ...

The Trust-e trustmark is an online branded symbol that signifies a Web site has made a commitment regarding its privacy practices. This privacy statement must necessarily disclose information about the type of information the site is gathering, the beneficiaries of the information (if any) and finally how the information will be used. The site agrees furthermore to display the trustmark and to be submitted to a review done by Trust-e official auditors.

---

[9] The connection to Internet can be established in different ways : dial-up connections via modem and telephone lines, ISDN connection and finally ADSL (Asymetric Digital Subscriber Line).

[10] Ainsi, notably Altavista (http://www.altavista.digital.com) ; Yahoo (http://www.yahoo.com) ; Excite (http://www.excite.com) ; Inforseek (http://www.infoseek.com).

[11] See about these risks, International Working Group on D.P. in Telecommunications (the so-called Berlin Group), Data Protection and search engines

[12] On Trust-e, see http://www.truste.org. A new letter is published and available on this Web site.

The consumer when clicking on the Trustmark have a direct access to the site's privacy statement[13].

Other « labels » are exist. We would like to underline that certain of these labels aim to cover a broader scope than the privacy issues such as the WEBTRUST label developed by the American Institute of Certified Chartered Accountant (AICPA) and the Canadian Institute of Chartered Accountants (CICA)[14]. On demand of a Website, Webtrust will review the website practices with the standards developed by Webstrust. These standards cover three fields : Consumer protection (prior information, warranties, recourse of the consumers, etc.). Security of the transactions and finally privacy questions. If the review is positive, the Webtrust trustmark is posted by the reviewers on the Website[15].

7. Another category of actors are « Cybermarketing companies » such as Double Click or IMGIS[16] which can insert unsollicited and appropriate advertising banners on a web surfer's screen. So far they are collecting data through the use of « cookies » and are establishing user'profiles band on logfile information and « cookies ».

Recently, J-M. Dinant[17] has demonstrated the functionning of the process put into place by the cybermarketing companies, qualified by this author as Not Trusted Third Party (N.T.T.P.).

« Firstly, the website affiliated to a cybermarketing company will incorporate an invisible link in its pages to the Cybermarketing Companies website. Secondly while loading the main page, the navigator program automatically and seamlessly opens a new HTTP session with the cybermarketing company. While requesting the included image, the navigation program communicates in his HTTP request header,

- the main page being visited (i.e. the keywords to search if the site is a search engine)
- the cookie already sent from the webserver or from the NTTP (Presently, there is no possibility for blocking the sending of these cookies) ;
- the type and language of the browser and of the OS ;
- the TCP/IP adress of the user.

When answering to the invisible link, the cybermarketing company knows

- the location of the ISP which (can be deduced from the TCP/IP of the user ;
- the language spoken and/or understood by the user ;
- the keywords typed on search engines (if the cookie has been collected through a search engine website;

[13] See for instance, the Privacy policy Statement published by America Online under the Truste Trustmark at http://www.aol.com/info/privacy.html.
[14] On Webtrust, see http://www.BennettGold.ca/webtrust ; see also,
[15] The Belgian, Dutch and French Institute of Accountants have recently decided to develop a label called Trust 2 which intends to ensure the conformity of the Websitepractices with the European regulatory requirements.
[16] More than 2.500 companies (very active in the electronic commerce e.g. Altavista) are affiliated to Double Click. About Double Click, see http : www.doubleclick.net/nf/general/oncooset, particularly the pages on Privacy (DoubleClick Privacy & Optout).
[17] See the multiple presentations done by J.M. Dinant summarized in Les invisibles sur Internet, Le droit du Cybersespace, Luxembourg, Summer Course, Proceedings to be published by NOMOS.

- the main page accessed by the netizen ;
- the last cookie of the netizen. The cookie can easily be an identification of the complete netizen's clickstream since many months insofar the life's duration is often more than ten years (!).

So before sending the image, the N.T.T.P. knows the cookie[18] value of the netizen. By « Cookie Value », one means the profile of the Web's user deduced from the different previous uses of the browser insofar their storage is permitted by the cookie[19].

8. Finally, one would like to point out a fifth category of actors : the software editor companies especially the browser editor like Microsoft or Netscape. It is absolutely necessary to take into account the technical features of the webbrowser in order to know exactly which flows are generated (e.g. the automatic sending of cookie) or allowed (e.g. possible hyperlinks without preliminary notice to the webusers)[20].

Recently, J-M. Dinant and myself have made certain suggestions and recommandations[21] in order to improve privacy protection at the brower's level. These recommandations are published in Annex 1. of this article.

9. In the context of the so called ECLIP Project, which has been launched by the Commission to study the legal aspects of the electronic Commerce and is presently developed by a consortium of five universitary research centers, we have tried to describe the different and multiple processing set up by the different actors and to identify for each processing the data stored and processed.

A first scheme does represent the processing performed in a normal electronic transaction.
So to summarize this first chapter, it is obvious that electronic commerce creates a number of privacy risks and for different reasons. Firstly, electronic commerce involves a number of different actors, located in different countries, including countries without data protection rules.

Secondly, these actors might collect data during the transaction or prior to the transaction, data generated by the user voluntarly or not, consciously or not and revealing their preferences or habits. Thirdly, certain actors have

[18] About the cookies and their functionning, see the article written by V. Mayer Schönenberger, The Internet and Privacy Legislation : Cookies for a Treat ?, CLSR, 14, n° 3, 1998, p. 166 et s. « Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, to allow users to participate in WWW-wide contests (but only once !) and to store shopping lists of items a user has selected while browsing through a virtual shopping mall ».

[19] This cookie can be related in teh NTTP local tables with the clickstream of the netizen. Because the NTTP knows the webpage being visited by the netizen (including the keywords of some searcher) he can add this valuable data in his table to keep an updated table. To keep clickstream tracks, it's only necessary that the netizen (or his son) have accepted one cookie one time.

[20] About these « privacy killers » features due to the present functionning of the browser, see the article published by Jean-Marc Dinant, http://www.droit.fundp.ac.be/crid/privacy/strenv.exc ?full.

[21] These recommandations have been presented before the so called art. 29 Working Group. This Working Group has been created by the European directive as a consultative Committee in order to adress certain reflections and recommandations to the European Institutions. It is compouned by representatives of the various Member States D.P. Commissions.

for obvious commercial reasons, great interest in exchanging among them solves the data collected by each one of them, creating a commerce of personal data.

Two additional remarks have to be adressed :

- the first one is the fact that according to different surveys[22] the Web sites are offering poor data protection. The US Federal Trade Commission has recently revealed that only 14 percent of the US commercial web sites are providing information about their data protection practices or policies.
- The second point to be underlined by the surveys is the increasing fear of the consumer about their online privacy. The Trust e Internet privacy Study asserts that more than 70 percent of the consumers are more concerned about their data protection in the Internet context than in traditional context[23]. It is quite clear that fair information practices as regards privacy has to be considered as a key element for the development of the e commerce[24].

II. Electronic commerce and privacy : a challenge for the regulatory solutions

10. Number of questions might be raised in that context. Perhaps, it would be possible to summarize these as follows :

- to what extent, the regulatory solutions (particularly the two directives, the General and the Telecoms ones) are challenged by the new data practices developed in the context of the use Internet techniques ?
- to what extent, through audacious interpretations of the regulatory framework, it would be possible to cover these new practices ?
- thirdly, would it be possible to use other legislations than those strictly connected with privacy questions, like telecom directives or consumer protection legislation in order to enhance privacy protection.
- finally, do we need concepts or principles in order to regulate Internet ?

A. The main challenges

11. As regards the identification of the challenges, the growing international or global character of the E. commerce and therefore the multiplication of T.B.D.F. underline the need to seriously take into consideration the provisions thereon (art. 25 Directive). What does « adequate protection » mean and which kind of contractual arrangements (Directive, art. 26) are we accepting in that perspective[25] ? Could we consider that

[22] See particularly, the survey done by OECD in April 98 (OECD, Group of Experts about privacy and Information Security, Projet d'étude sur les instruments et mécanismes relatifs à la mise en œuvre sur les réseaux globaux des lignes directrices de l'OCDE sur la vie privée)n the F.T.C. Survey conducted in March 98 (published at : http:// www.ftc.gov/repats/privacy3 :survey.htm) and the EPIC study published at http://www.epic.org/reports/surfer-beware.html (study conducted in June 97).

[23] The Trust e Internet privacy Study has been conducted by the Boston Consulting Group in March 97 published at http://www.truste.org/webpublishers/studies_BCG.html).

[24] The Trust-e Study quoted above points out that 42 % of the consumers refuse any registration informations and that 27% are giving false informations.

[25] On that point, see the study done for the Commission, Y. Poullet, B. Havelange, A methodology to evaluate the « adequate protection » in the sense of the art. 25 (Privacy Directive), to be published by the Commission.

notwithstanding these provisions, European judge might argue that « privacy protection » is of international public order and so deny any application of less effective foreign data protection ?

12. The multiplication of intermediairies in the data flows generated by E. commerce (see supra n°3 and ff.) underlines the need to regulate their liability in case of privacy infringements of websites. Does the future directive about the liability for online services provide an adeqaute solution in that sense ? In that perspective, it has been underlined that the « reasonable » means to have knowledge of privacy infringements and to avoid them, not only on a curative but also on a preventive manner, must be defined. The concerns about the fear of an « overcensorhip » practised by the intermediaries and about the need to have « recourse » possibilities forued web sites before « independant » magistrates have been expressed.

13. Finally, the interactivity of the network does suggest an increasing role of the consent. The web user is enabled at each moment to remain or not anonymous, to interrupt or not a website's visit, to refuse or not the delivery of certain data, to accept or not certain practices, etc. All these possibilities suppose the respect of a free, explicit and informed consent. In this regard, a lot of questions might be raised : to what extent, can we consider that the web user is informed in case of publications of the privacy practices on a F.A.Q. webpage. Is the consent free, if the website in a quasi monopolistic situation, does not provide other solutions than the sending of proportionate data to obtain the service proposed. How, can one be sure that the consent is explicit as regards certain characteristics of the processing (e.g. the processing is requiring transforder data flows or is pursuing different purposes presented as an individable block) ?

Still as regards the consent, can one consider that the consent might in any cases, be considered as a legitimate ground for a processing. The question is quite important not only as regards sensitive data but also in consideration of the new protocol for privacy Preferences (P3P) developed by the W.3. consortium[26] and to be submitted in the next months to the Internet Society.

The P.3.P. conceives privacy and data protection as something to be agreed between the Internet user, when data are collected, and the website that collects the data.

The mechanism of this agreement is simple : the internet user is invited to define his privacy preferences. These privacy preferences are embodied in the browser in such manner that the user will be connected automatically only with the website which declare privacy practices satisfying these privacy preferences. If a website does not satisfy with the privacy's requirements of the user, there is a place for a negociation between both them.

The main ideas of the study have been taken again by the Art. 29 W. Party in the document recently adopted Transfers of Personal Data to Third Countries- Possible Ways forward in Assessing Adequacy.
As regards the application of respectively art. 4, 25 and 26, see C. de Terwangne, S. Louveaux, Internet and Privacy, C.L.S.R., 1996.

[26] That is to say the consortium formed by three prestigious research centers : MIT (U.S.), KEYO (Japan) and INRIA (Europe-France). About the P.3.P. harmonized Vocabulary Description, http : // www.w3.org/TR/1998/WD. P3P harmonization.

This negociation might lead a person disclaim his privacy requirements in favor of financial incentives (e.g. discount on the prices) and give his consent to unacceptable processing.

On that point, N. Platten[27] recently does claim the question if these financial inducements to provide data will not create a two tier society between rich people which will have the possibility to remain anonymous and poor people which will have to provide multiple data to get the services at affordable prices.

B. Towards an audacious interpretation of the D.P. directives

14. It has been argued by different authors[28] that an extensible interpretation of the Data Protection legislation's concepts and provisions might solve number of the new privacy threats created by Internet and its environnement.

The reader will find in Annex 2 the comprehensive study done on that point by Sophie Louveaux and the numerous examples contained therein. Our intent is solely to point out certain of these possible interpretations.

15. The first one is definitively the problems of the « cookies ». One knows the argument given notably by the Cybermarketing companies asserting that with cookies, they have knwoledge only of the browser identification number and not of the name of the person behind this number and they ensure that never they will try to identify this person. Therefore, they consider that their processing is outside the scope of the data protection legislation.

In order to fight this argument, we point out the fact that, even if the identification of the web user is technically impossible. the use of cookies to sketch user's profiles (what a web user is doing) in order to send him the appropriate advertisement creates « personal data » inso far they identify the person by reference, as the directive asserts, to one or more factors specific to his « physical, psychological, mental, economic, cultural or social identity ». This counter argument might be reinforced by the simple reflection following which a marketing company in the traditional world (that is to say in the non electronic and virtual world), is more interested in a potential customer's profile than to his identification as physical person. This identification is only needed in this traditional world for contacting him by post or by phone. If this identification is no more necessary as it is the case in the virtual world (I can adress the advertisement automatically without knowing the physical characteristics of the person – address, name, etc.), it is quite clear that the data collected for determining the user's profile have to be viewed as personal data.

16. A second example is the extension of the scope of article 14 of the D.P. general directive and of article 12 of the D.P. Telecom directive about the right of the data subject to refuse (system of opt out) the unsolicited calls and the use of his data for marketing purposes.

---

[27] N. Platten, Privacy enhancing technologies, Panacea or deception, 1st ECLIP Seminar, Namur, 1998, (http://www.droit.fundp.ac.be).

[28] See on that point, the noticeable study done by C. de Terwangne and S. Louveaux, already quoted and my article. Internet et Vie Privée : nouveaux enjeux, nouvelles solutions, colloque de Strezza, Giuffre, Milano,

In our opinion, this right to object is applicable also in the Internet context. So, article 14 b. could serve as ground to prevent automated hyperlinks to cybermarketing companies in the same way as article 10 of the Telecom Directive grants subscribers with the possibility to stop automatic call forwarding.

According to the same argument, article 12 § 2 of the Telecom Directive applies to unsolicited E mail messages however the term « unsolicited call » suggests that the provisions only cover phone calls. Indeed, so far the aricle 12 § 1 provision asserts unambiguously that fax messages are « calls » in the sense of article 12. We might consider that an email message is also a call.

17. The last example is the application of article 4 1. C) of the directive in case of transborder data flows generated by the non visible processings created by the use of cookies placed by companies located outside Europe on the webrowser of a user located in Europe. The problem is the following. If hidden flows deriving from cookies are transborder data flows, that is to say flows towards countries ouside Europe, must we apply article 25 and 26 or article 4.1. c) ? If the first solution is choosen, we will have to analyze if the protection afforded by the company in the third country is adequate. If we take into account the second solution, the company even if located outside Europe will have to comply with the European principles (and notably, the duty to inform the data subject about the processing and its characteristics will be imposed).
In our opinion, in case of cookies, the controller of the processing (the sender of the cookies) « makes, taking again the wording of article 4.1.c), use of equipment situated on the territory of a Member State » insofar as the cookie is inculcated in the Webbrowser of the webuser and is sending automatically and seamlessly the data to the cookies's sender.

C. Beyond privacy regulations

18. It is noticeworthy that other regulations than privacy regulations (in the strict sense) might be helpful to protect the webuser against privacy infringements. It has been suggested that « consumer protection » regulation might also be of some help to solve privacy problems. The main interesting example is the « liability for defective products » directive. To what extent, a webbrowser allowing certain privacy infringements as the cookies'reception and sending without prior notice is a « defective » product. Other interesting remarks might be deduced from the « distance selling » directive as regards the right of the Web user to object to unsollicited e-mail messages and the duty of the Webuser to deliver informations about his identity[29].

An other trail might be followed founded under the Telecommunications regulatory framework. One knows that « privacy protection » is one of the essential requirements to be checked to approve terminals equipment. To what extent, would it be possible to regulate the technical features of the web browser (e.g. automatic sending of cookies) on that legal basis ?

1998, 49-72. More recently, the study done by the italian representatives at the art. 29 WG, Implementation of Directive 97/66/EC with respect to Internet Services, Doc. XV/5024/98.E N.

[29] See art. 4 § 1 of the Directive on the Protection of consumer in respect of Distance Contracts (20/5/97, O.J.E.C., L. 144, 4/6/97).

D. Towards New Data Protection Principles ?

19. The widespread use of new technologies of information and communication which is the main characteristic of the electronic commerce does suggest new data protection principles. To new risks must correspond new concepts and new principles in order to ensure correctly the protection of the individuals[30] data.

The recent German Act[31] implicitely consecrates four new principles which seem also be enacted in other recent recommandations and regulatory texts.

20. The first one is definitevely the « data minimization ». This principle mean that the data controllers must process the minimum data required to ensure the proper performance of the processing.

21. The second one is the right to remain anonymous[32]. This right has been expressly enacted in different regulations on electronic signatures[33]. The right to use a pseudonym instead of ones official name is fundamental.

The European Working Party, the so-called Article 29 W.G.[34] has also clearly asserted the right to use the web anonymously and more recently the Council of Europe has recommended[35] that the Internet providers inform the web users about the possibilities of accessing the Internet anonymously, and using its services and paying for them in an anonymous way (e.g. free paid access cards).

---

[30] Perhaps, these new risks will require the extension of the data protection provisions to legal persons. Thereabout, it is interesting to notice that the Telecom directive ensures a data protection also for legal persons. So far the Telecom Directive is broadly applicable in the Internet context to processing held by different actors like Internet Access Providers, Internet Services Providers and obvioulsy Telecommunications operators, that means that legal persons might claim the benefit of data protection vis-à-vis these actors.
This remark leads to the question about the opportunity to extend more generally the Data Protection regulations vis-a-vis the legal persons and not only to individuals.

[31] « The provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed about these options » (Art. 2, § 4, Law for Information and Communication, IukDg, 13 June 1997, BGBL, I.S., 1997 , 1870).

[32] As regards the implementation of this right to anonymity, see Privacy – Enhancing Technologies : the path to anonymity, vol. I and II, Report done and published by both Registratiekamer (NL) and Privacy Commission (Ontario/Canada), August 1995.

[33] Proposal for an European Parliament and Council Directive on a common framework for Electronic Signatures (13/5/98-COM(98) 297 final).

[34] « Anonymity on the Internet », adopted by the Working Party on 3 December 97. (See also, the Report and Guidance by the International WG on Data Protection in Telecommunications (« Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet). « On the key issue of anonymity the same approach should be taken ... the principle should be that where the user can choose to remain anonymous off line, that choice should also be available on line ». « The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line ».

[35] Council of Europe, Project Group on Data Protection (CJ-PD), The protection of privacy on the Internet, 35th meeting, Strasbourg, 25-27 March 98.

Moreover, must pointed out the suggestion of the OECD group of Experts asserting that the commercial web sites must offer as regards the payment of low amounts, anonymous ways of payment[36].

Finally, the right to anonymity has been involved to justify the possibility for a person to register not to have his data displayed as a search result (the no-robot option)[37].

22. The third principle is the « integration of the functionnalities of the technology » in order to implement the data protection principles. The applications of this principle are various and noticeworthy. It means that each time, the same technology as that used for collecting or processing data might be viewed as a way to implement or even to enhance the data protection principles, the technology must be configured in that sense. So, the right for the webuser to be correctly informed about the website privacy practices might be implemented through website pages placed at the forefront of the website or by hyperlinks to the codes of conduct respected by the website[38].

The right for the webuser to have access to his own data or to object to processing for commercial purposes might (op-out) be exercised electronically.

According to the same principle, one can imagine that through certain labels (no robot[39], no spam[40]) the webuser might automatically forbid the use, on the one hand of his name, as keyword for search engines or, on the other hand, of his email adress for the sending of unsollicited email.

A lot of other examples might be given, particularly as regards the possibilities to ensure a free, explicit and enlighted consent by technical means.

An other meaning of this third principle implies that the Internet Software, particularly the browser, must be configured by default in such a way that the maximum of privacy protection is enabled[41].

23. The fourth principle is the « electronic enforcement of the legal position of the person concerned », that means that a certain number of initiatives must be taken in order to make transparent and enforceable through on line techniques, the multiple rights of the webuser. Beyond what has been already under the 2d principle, it must be ensured that the access to the official or non official data protection authorities in case of complaints will be granted through automatic means.

---

[36] OECD, Group of Experts about privacy and Information Security, Projet d'étude sur les instruments et mécanismes relatifs à la mise en œuvre sur les réseaux globaux des lignes directrices de l'OCDE sur la vie privée, OECD, Paris, 18-19 may 98, Suggestion n° 25.

[37] Int. Working Group on Data Prot. in Telecommunications, Data Protection and Search Engines on the Internet, Report and Recommandations, Hong Kong, 14-15 April 98.

[38] See on that point, the suggestions n° 17,18, 20 and 21 of the OECD Group of Experts which claims that the « privacy Statements » of the web site clearly identified on each web page and accessible on line to the web users and that are hyperlink to the code of conduct or to the D. Protection authority web site must be provided.

[39] On that point, see supra n° 4, note 3.

[40] On that point, about unsolicited email, supra n° 17.

[41] See our recommandation published in Annex 1.

Insofar as a public registrer containing the notification of the practices exists (article 17 of the Directive), a hyperlink to this public registrer must be integrated and a clear indication of this possible hyperlink has to be indicated in front of the website. So the web user might automatically have a view on the content of the notification made by the webiste data controller or, in case of a missing hyperlink, the user will know that no notification has been made[42]. Another interest of this proposal is the fact that this hyperlink might be withdrawn if the website practices no more comply with the practices notified.

Finally, vade-mecum explaining the privacy risks, the privacy duties of the website data controller and the rights of the webuser as data subject must be broadly diffused including through Internet and the Data Protection authority must be present on the web through an interactive, documented and updated website[43].

III. Some considerations about self regulation and privacy enhancing technology

The debate between partisans of the self regulatory approach and the legislative approach is often viewed as the debate between American culture and European culture. It is quite obvious that this dichotomy approach obviously does not exclude intermediary solutions privileging a dialogue between these two regulatory ways[44].

The selfregulatory approach does encompass different tools :

- the technical ones the so called PETS[45], as P.3.P., cryptographic methods, Cyberpatrols, Identity protectors, etc.
- the labelling of the website like Trust-e[46] or other labels having a broader scope than only the respect of the privacy requirements (WebTrust, Trust 2)[47].
- Finally, the Company's privacy policies or the codes of conducts developed on a sectorial or multisectorial approach.

---

[42] This idea has been developed by the Belgian Data Protection Commission.

[43] The CNIL's site is examplar on that point.

[44] Art. 27 § of the General D.P. directive establishes clearly a classification of rules according to the priority a rule should have towards the others. Under art. 27, Code of conduct that is to say self regulatory solutions might be seen as complementary way to chieve and reinforce the implementation of legislative solutions : « The Member States and the Commission shall encourage the drawing up of Codes of conduct to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking into account of the specific features of the various sectors ».
The recent american debate before the Federal Trade Commission illustrate another approach. The Federal Trade Commission recommands that the online industry will be regulated by the Government unless it adequately protects consumer privacy by January 99. So, the legislation is viewed as a possible sanction in case of unsuffisiency of the selfregulation solutions. « Unless industry can demonstrate that it has developed and implemented broadbased and effective self regulatory programs by the end of the year, additional governmental authority would be appropriate and necessary, said Pitofski in Testimony prepared for his appearance before the House Subcommittee on Telecommunications, Trade and Consumer Protection ». (See on the F.T.C. debate : http://www.wired.com/news/news/politics/privacy/story/13895html.

[45] The acronym « PET » (Privacy Enhancing Technology) has been created by the famous report issued by both Dutch and Ontarian D.P. Commission. On the PETS and their value, see H. Burkert.

[46] About Trust e and other labelling mechanism, see above n° 6. About the labelling practices for privacy protection, see E. Dyson, Labelling practices, in Privacy and Self regulation in the Information Age, US Depart. of Commerce, NTIA, June 97, p. 183 and ff.

[47]

A. Preliminary remarks

24. Certain remarks must be adressed before proposing a list of criteria in order to evaluate PETS and self regulatory solutions.

About the P.3.P., beyond remarks about difficulties to have a good terminology and a sufficiently sophisticated system to encompass all situations, more fundamentally it might be underlined that the shift from regulatory a priori solutions to the contractual paradigm (everthing is negiotiable) does represent a real danger for privacy. Moreover one can assert that a « Human Rights » approach, that is to say the fact that Data Protection is a constitutive element of a democratic Society, implies the need to ensure Data protection by legislation. That conclusion does not mean that PETS (or self regulation) are not interesting as complementary ways to protect privacy but they can never be viewed as a substitute.

An another remark is founded on the multiplicity of self-regulatory solutions which can be the source of conclusion for the web user. Therefore, it has been pleaded in favour of a common European label. The D.P. authorities would be envolved in the procedure for defining the label's requirement in order to assess the compliance of these self-regulations with the D.P. principles.

B. Criteria to assess the quality of the technical or selfregulatory measures for Protection of Privacy

25. The reflections laid down hereinafter aim to propose three criteria in order to evaluate the non regulatory privacy measures derived or not from a legal framework. As it will be underlined, it is quite clear that these criteria will be different in these two context. In the first case, the self regulation must be viewed as an ancillary way to protect privacy and the most important question will be its compliance with the legislative requirements as expressly provided by article 27 of the Directive. In the second case, the self regulation is a « substitute » and the question is then « Is this substitute offering an « adequate » protection to take the word used by article 25 of the Directive ? ».

Anyway, in both cases, the assessment of the code of conduct will have three criteria[48]

- legitimation as regards the authors of the code ;
- conformity as regards its content ;
- effectiveness as regards its enforcement.

The three cirteria are explicited as follows.

a. The legitimation

[48] About these criteria to assess the adequacy of a protection, our reflection in Y. Poullet, B. Havelange, A Methodology for the Assessment of the « adequate protection » in the sense of article 25 of the Directive, Report done by the CRID for the European Commission (DG XV), to be published by the European Commission.

26. The first question to be risen concerning a self regulation is the legitimation of its authors ! Who is promulgating the code of conduct ? Who has defined the technical standards ? To be more precise : after which kind of procedure has the self regulatory mechanism been adopted. In our opinion, a self regulation might be acceptable only if the opinions of all interested parties (that means not only the data controllers' representatives but also the data subjects' points of view) have been taken into account. The involvement of all interested parties might be ensured through different ways (e.g. by public hearing) but in any case it must be checked if the procedure used to adopt the self regulation was from this point of view, sufficiently open and transparent. This requirement is absolute in case of non existing legislative framework.

b. The conformity

27. To what extent, a self regulation instrument is complying with the D.P. principles ? This question is crucial. Indeed, what will be checked by the auditor in case of demand of a privacy label addressed by a web site data controller ? What does it mean in case of technical standards to be a privacy complying technique ? In the case of existing legislation, this examination of conformity's might be simple but in the other cases, the solution to this question is rather intricate. However, one might consider that certain certain D.P. principles are internationally recognised :

1. The data subject's right to be informed, his right of access and rectification[49] ;
2. The purpose limitation and the need for a social justification ;
3. The data proportionnality ;
4. The security measures' requirement.

c. The effectiveness

28. Compliance with data protection principles and legitimation of the authors are not sufficient. The third criteria intends to measure the effectiveness of the selfregulation. Three subcriteria might be distinguished on that point.

- the awareness and userfriendliness of the selfregulation

Questions like the broad (or not) publicity and the easiness of access to the content of a code of conduct, as the userfriendliness of privacy enhancing technologies (e.g. Is the blocking of cookies' a time consuming operation ? Are the anonymisation's techniques easy to use) must be raised. In case of PETS, the problem of their costs and their availability on the market for a webuser must be checked attentively.

- the accessibility, quality and investigation powers of the controllers

It is quite important that the authority in charge of the respect of the self regulation might be easily accessed by the web user, at a affordable cost or better free of charge, that this authority is neutral and can act independantly of the data controllers. This authority must be equiped with real powers of investigation and finally, its dealings must be transparent (for example, via a report accessible to the public by the publication of its decisions)

49

- the need for effective sanctions

It is quite clear that nother sanctions than the penal ones might be envisaged and are often more effective, like the blocking of a website, the withdrawal of a label, etc. The only criterion must be : are the binding sanctions promulgated by the self regulation sufficiently deterrent to prevent the non respect of the D.P. principles ?

The american GeoCities case (GCTV)[50] is an example in that perspective. Two days after is extremely successful initial public offering, GeoCities Inc. (GCTV http://www.geocities.com) settled with the U.S. Federal Trade Commission regarding a complaint that it betrayed its customers by revealing their private data to Web advertisers. Under the terms of the settlement, GeoCities must post a clear notice on its site revealing how it will use consumer information, and it must make the information available to users for removal at their discretion. Moreover GeoCities must provide free email services to the public in order for its customers to address their complaints.

One underlines that through this settlment before the F.T.C. The U.S. Government enforced the Internet privacy policies, asserting that GeoCities had not respected the right of its customer to be informed and his right to opt out in case of use for marketing purposes.

The most interesting feature is perhaps that this government intervention costs GeoCities millions of dollars inso far as on the Stock Market the GeoCities shares dropped as much as 22 percent in two days.

Conclusions

29. Recently, I was told by an American friend in a provocative manner : « In Europe to regulate Internet, you have nice legislations, you have created bureaucratic data protection authorities but amongst the population, there is no privacy concerns and the protection you are offering is purely theoritical. In US, the privacy concern is very high, we have effective selfregulation and technical tools have been developed to solve the real problems ». This assertion is partly true. On the one hand it is quite clear that a legislation without self regulatory and technical satisfactory solutions will only serve as window dressing but on the other hand without a legislation or without the fear of a legislation (in that context, the PICS'development as a way to avoid the american Decency Act is a good example), it is not certain that selfregulatory solutions will be imagined and adopted and that their content will be adequate to ensure privacy protection.

We should like to stress the State's vital obligation to intervene at a time when, in our opinion, deserting the Internet and withdrawing from the field of regulation to such a point that it no longer even decides the general framework, would notably put at risk public order, fundamental liberties and other basic values[51].

---

[50] http://www.geocities.com

[51] As recently asserted by the U.S. Vice President Al Gore in our address to N. York University. « We need an electronic Bill of rights for this electronic age. You should have the right to choose whether your personal information is disclosed ; you should have the right to know how, when, and how much of that information is being used ; and you shoud have the right to see it yourself to know if it's accurate » (White House Briefing

30. The role of the State vis a vis the development of the technical standards and in general of the selfregulation is of crucial importance. Through specific legislation, the government has to encourage the development of technical tools complying with privacy requirements (e.g. in Belgium, we are thinking about a legislation granting certain legal advantages to web sites voluntary accredited). Furthermore, the government might provide research funds in order to develop the needed technical tools and decide to implement them for itself, notably in the relationships between administration and the citizen, the fair information practices and privacy enhancing technologies, he has contributed to develop.

31. Finally, the government has to ensure a better awareness among the citizens about risk to privacy of Internet and about the adequate solutions, the technical tools and the interactivity the network provides. It is quite clear that the internet user is himself his best identity protector. He might decide to prevent the arrival of cookies, to erase them or block their sending ; he might, through techniques of encryption or of anonymisation, protect the confidentiality of his message or its anonymity ; he might reveal or not certain data, decide to communicate only with rated websites and use his access right to control their activities.

Room Media Release 31 July 1998.www.usia.gov/products/washfile.htm). During the speech, Al Gore called for immediate actions s regards sensitive personal information (particularly medical and financial records) and to protect children's privacy online by ensuring that data is not collected from children without parental consent.